1) TIGHTEN INTRO
2) CONDENSE/ SIMPLIFY HISTORY PART

Joshua S. Gottheimer
07/10/2000 07:39:25 PM

Record Type: Record

To: Mara A. Silver/WHO/EOP@EOP

cc:
Subject: this is about 500 words too long

Draft 07/10/00 7:30pm
Gottheimer/ Swire

CHIEF OF STAFF JOHN PODESTA
REMARKS TO PRESS CLUB ON ELECTRONIC WIRETAPPING
WASHINGTON, DC
July 14, 2000

LONG STANDING SHATTERED BARRIERS OF TIME AND SPACE OR SOMETHING -- TAKE OUT "KEPT US APART"

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he broke down geographic barriers th~~at had long kept us apart~~, opening up a world of possibility that was never even imagined just a few years before.

Morse's invention set in a motion a technological revolution that would forever change the way man would communicate. Only a few years later, in 1858, Queen Victoria bridged the waters of the Atlantic, when she sent the first transatlantic telegraph to President Buchanan in the White House. Just two decades later, using a funnel, a cup of acid, and some copper wire, Alexander Graham Bell invented a device to give~~a person~~'s voice -- not just his words – a way to travel.

THIS JUMP TOO MUCH: COMMUNICATION → GENOME → INET

SOUNDS AWKWARD B/C YOU WERE TALKING ONLY OF COMMUNICATION TECHNOLOGY

TODAY,

Today, the great revolution in ~~science and technology~~ communication tech continues. Just last month, we announced a major breakthrough in science – the completed map of the entire human genome. With this map in hand, ~~we could~~ gained the pwr to one day eradicate ~~many~~ some of the most deadly diseases known to man. ~~That map wouldn't have been possible without the~~ computers and shared information over the Internet. Fr~~om small towns to big cities~~, the Internet is bringing millions of people ~~closer together~~, giving them new ways to find information and to stay in touch. When it was invented ~~just~~ thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a reservoir of information – from Shakespeare's first sonnet to the remarkable photos just taken of Mars.

I WOULD STICK W/ OOH AHH COMMUNICATION STUFF MAKE BETTER TRANSITION FROM TELEG/PHONE → INET

IN COMM. TECHNOLOGY

¶ BUT ~~This new potential also brings new risks.~~ IT Because we are so interconnected, more people now have easier access to our most personal information – from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

*PUT ABOVE

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our ~~most fundamental~~ values – and the need for new laws and new protections to maintain them. Over the last seven and a half ~~years, our~~ Administration has taken steps to keep our laws and policies in line with the latest advances in technology. To combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. Just this February, in his Cyber Security Summit, the President emphasized the role and responsibility of the private sector in implementing computer and network security. We've also worked to develop strong encryption tools – like those implemented in the by the European Union -- to provide tighter security and privacy in election communications.

Additionally, we've taken steps to ensure that the appropriate cyber security measures are included as part of all government computer systems. Unfortunately, Congress has not given us the necessary funding the President has requested to take additional steps, such as funding an internal expert review team. And we've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. As Supreme Court Justice Louis Brandies once said, "Time works changes ... [it] brings into existence new conditions and purposes." ADD SENTENCE FROM CONTEXT

Today I want to talk to you about another step we should take to keep our nation's laws consistent with the latest advances – the updating ~~and harmonization of existing wire tapping~~ laws. ~~The fundamental debate over~~ these laws is rooted ~~in the Fourth Amendment~~ of the Constitution, which states: "The right of the people to be secure in their persons, houses, ~~papers, and effects,~~ against unreasonable searches and seizures, shall not be violated."

In 1787, a person's most important "papers and effects" -- like diaries and letters -- were almost undoubtedly in their home or place of business. Our "papers and effects" were thus protected by the requirement of a warrant before the state could enter and search. But with advances in technology, people no longer relied solely on paper and pen to communicate with one another. By the turn of the 20th Century, people were using the telephone for personal calls and business transactions. And today they're relying on the Internet. Over the years, this has forced a debate in Congress ~~and~~ in the Courts over the application of the Fourth Amendment: — THAT "THE RIGHT OF THE PEOPLE..." Quote

(ITALICIZE)

In the 1928 Olmstead case, the Supreme Court found that conversations over the telephone were not protected by the Fourth Amendment, and therefore wiretapped conversation could be submitted as evidence. Judge Brandeis disagreed and argued that, "There is, in essence, no difference between the sealed the letter and private telephone message." ~~And the Supreme Court had held in 1877 that sealed letters and packaged couldn't be opened by postal~~ inspectors without ~~a judicial warrant~~. Wiretaps~~, Brandeis argued, invaded the privacy of~~ people on both ends of the ~~line, exposing far more intimate activity than warrants in the 18th Century~~. That, he ~~recognized, was~~ privacy the framers ~~intended to protect~~ with the Fourth Amendment.

CONDENSE

The 1968 Court agreed with Brandeis, when it ruled in *Katz vs. the United States* that an individual's phone conversation was protected by the Fourth Amendment, and therefore inadmissible in court proceedings. Later that year, Congress responded to the decision by passing new legislation with strict standards for all wiretaps. Among other things, Title III of the Crime Control and Safe Streets Act required a court order and high-level Justice Department approval for all wiretaps. Its provisions only allowed wiretaps for the most serious cries, such espionage, treason, and crimes of violence; and it required detailed annual reports on the number and nature of all taps. Most importantly, Title III stated that any information attained outside the parameters of the law was inadmissible in court.

CONDENSE AND MAKE SIMPLER

Title III remained relatively untouched until the mid-1980s, when cellular telephone service, e-mail, and other computer-to-computer communication put new demands on outdated provisions of the 1968 privacy law. Like the phone in the 1920s, the new electronic technology of the 1980s raised new questions~~, which~~ that required new solutions. ~~Most notably~~, Title III of the 1968 law only applied to wire and voice communications – not to wireless phone conversations or e-mail. By ~~that year~~ 1984, there were more than 7,000 Americans using cell phones, and more than 400,000 using electronic mail. ~~In fact, by 1984, the Internet itself had grown to 1,000 users~~.

In response, under the leadership of Senator Leahy, Congress adopted the Electronic Communications Privacy Act of 1986 -- once again updating its laws to keep pace with changing technology. Before ECPA, the government could use an electronic wiretap to monitor an individual's e-mails with a ~~just a~~ mere subpoena. ECPA changed that, and put in place many of the protections the courts had delivered to phone conversations two decades earlier.

ECPA did several things: it made clear that wireless voice communications were covered tot the same degree as wireless voice communications. It extended some, but not all, ~~of Title III's~~ privacy protections to electronic communications intercepted in real-time. It also set standards for access to stored email and other electronic communications and transactional records, and adopted the trap and trace statute, governing real-time "interception" of "numbers dialed on a phone line." Just as it had been a federal crime to intercept telephone conversations since enactment of Title III, ECPA made it a federal crime to intercept electronic mail, data transmission and other electronic communications. This was a big step, and one that was sorely with the advent of electronic communication.

But ECPA – like its predecessors – has, in many ways, become outdated by new advances in computer technology and electronic communication. Our ~~country, and the~~ world is increasingly more digital – increasingly more interactive. Since the passage of ECPA, we've seen ~~the mass~~ A COMMUNICATIONS REVOLUTION W/ THE CELL PHONE AND THE rise of the development and use of the World Wide Web.

Today there are more 360 million cell phone users, and more than 50 million households on line in the United States, that's an increase of ~~over~~ 1250% since 1984 alone. And more than over 1.4 billion e-mails change hands each and every day. Moreover, computer users today don't just send message through their external modems, nor do they store

IF YOU NEED TO YOU COULD CUT THIS OUT

information on their computers the way they did in the 1980's. Now many of them send e-mail through web sites like Yahoo, or through Internet service providers, like AOL; and they download files and e-mails on to servers at work and at home. And a growing number of Americans – 2.2 million – log on to their e-mail through cable modems, a means of connection that wasn't even considered in ECPA. ~~In fact, until the late 1980s, no one even thought that the cable going into your home would be used for anything but television programs. To protect the privacy of home viewers, the cable laws passed in 1986 made tapping a cable line even more difficult than tapping a phone call.~~ END CUT

ECPA was not devised to address many of the issues related to these newer, faster means of electronic communication. ECPA does extend full ~~Title III~~ protections to email sitting on the server of an Internet Service Provider – like those in Yahoo's corporate headquarters in Santa Clara, California. It doesn't include other protections – like the scope of crimes covered, ~~and~~ the need for high level ~~Justice Department~~ approval, ~~and judicial supervision.~~ + oversight. And ECPA doesn't include a statutory suppression rule for government violations, or a mandate for annual reports.

THIS GOOD ... MUCH CLEARER

What does this mean? It means that data stored on networks is not afforded full privacy protection. That many of the protections in the wiretap law do not apply to email and other Internet ~~protections~~ services Americans so often use. That ISP customers are not entitled to notice when personal information is subpoenaed in civil lawsuits. And that inconsistent standards apply to government access ~~to~~ information ~~depending on the type of technology used~~.

Basically, the same e-mail sent ~~via cable TV, Internet cable modem, and ISP are all~~ in different ways is subject to different privacy standards. Considering the extent to which our electronic correspondence contains our most sensitive thoughts and information -- shouldn't they count as the "papers and effects" mentioned in the Fourth Amendment? It's time to adopt legislative protections that map Fourth Amendment principles onto the latest technology. It's time to update and harmonize our existing laws to give our e-mails, over ~~ISP servers and cable wires~~ all forms of technology, the same legislative protections as our telephone conversations. I propose the following steps:

Suggestion

First, some current statutes apply to criminal who use hardware "devices" but not to identical crimes that use software instead. Such telephone-era laws should be clearly updated to apply to an Internet era where hardware and software are interchangeable. In our proposed legislation, we ~~should~~ would amend statutes that are hardware-specific or use 'devices" and other outmoded language. We ~~will~~ would also continue to study whether any additional legislative responses are appropriate to distributed denial-of-service or other new threats.

Second, we need to achieve *harmonization* of how the laws apply to different forms of communication. As I mentioned, the current law sets stricter standards for law enforcement access to "wire" communications such as telephone calls than for "electronic" communications such as e-mail. In our era of rapid technological change, one of ~~the~~ our Administration's central ~~principles has been~~ *technology neutrality* -- the idea that the government and the laws should be generally neutral ~~between different~~ technologies. The market should play the central role in picking technological winners and losers, not Congress or the regulators.

THIS WOULD BE IMPT TO SAY ABOVE AS INTRO TO ~~DOJ~~ HIS SUGGESTIONS

In order to achieve this neutrality, we propose to harmonize the legal standards that apply to law enforcement access to e-mails, telephone calls, and cable services. For more than 30 years, federal law has set a tough, but manageable standard for when law enforcement officers can listen to the contents of phone calls. ~~Today, when e-mail and other "elec~~tronic" Email deserves comm~~unications are relied upon similarly to phone calls~~, AWKWRD ~~we believe that~~ the same legal protections ~~should ap~~ply. These protections include high-level approval within the Department of Justice, ~~use~~ only for the most serious crimes, and suppression of evidence in court if the rules are not followed. as for the telephone.

At the same time, we propose to change the standards that apply to cable services. Under the current Cable Act, even where there is clear proof of serious crimes, law enforcement officials cannot gain access to subscriber records -- unless the customer first can contest the issue in court. With our proposal, we would retain the underlying purpose of the Cable Act to keep confidential the list of shows that a customer has watched. But, when cable systems are used to access the Internet, we believe the rules should be the tough but manageable standards we also support for e-mails and telephone calls.

Third, we need to seek *balance* among crucial goals -- including the protection of public safety, the achievement of economic growth and digital opportunity, and the preservation of privacy and civil liberties. That's a challenge that our forefathers grappled with when they wrote the Constitution, and one that our government and courts have struggled with ever since. Our aim should be to enhance law enforcement authorities ability to address unlawful conduct, but also to enhance privacy and civil liberties on the Internet.

For example, we need to update the longstanding legal rules that govern when law enforcement can track the identity of those with whom we communicate. Our "trap and trace" rules come from the era of the traditional telephone network, when one company offered nationwide phone service. Telephone service today is offered by a bewildering variety of companies that offer local, long distance, and wireless services. Tracing a phone call often requires separate subpoenas in the various courts where each of the companies operates. The problem in tracing Internet communications to their source can be even worse. The structure of the Internet means that communications are routinely shuttled among many nodes, often in different federal court districts.

Today, we are proposing ways to make these "trap and trace" rules more effective for law enforcement, while also better assuring privacy and civil liberties. We believe that a federal court should be able to issue one order to trace a communication to its source, and that order should be effective nationwide. We also believe that there should be greater judicial oversight of trap and trace authorities. Federal law should make clear that such orders should only be issued after a judicial officer has determined that the proper factual showing has been made.

In the early years of our republic, Thomas Jefferson said, "America's institutions must move forward hand-in-hand with the progress of the human mind." Today, the progress of the

AWESOME QUOTE

DIF'T WORD

human mind is certainly racing forward at break-neck speech. Technology is opening up a new world of possibility -- but it is also challenging our privacy in ways we might never have imagined. In the right hands, the computer has become an indispensable tool for education, business, research and development. But in criminal hands, the same computer becomes a tool of destruction. As in any era of great progress, we must work together to ensure that our democracy and our laws keep pace w/ our minds -- and that we protect our civil liberties, not just the law enforcement mechanisms that were instituted to preserve them.

person's associations, habits, contacts, interests and activities. (Extending this to email and other electronic communications can, as we explain below, be even more revealing.)

In 1986, as cellular telephones service became available and email and other computer-to-computer communications were developing, this Committee recognized that the privacy law was woefully out of date. Title III anachronistically protected only wire and voice communications: it did not clearly cover wireless phone conversations or email. In response, under the leadership of Senator Leahy, Congress adopted the Electronic Communications Privacy Act of 1986 (ECPA). ECPA did several things: it made it clear that wireless voice communications were covered to the same degree as wireline voice communications. It extended some, but not all, of Title III's privacy protections to electronic communications intercepted in real-time.

ECPA also set standards for access to stored email and other electronic communications and transactional records (subscriber identifying information, logs, toll records). 18 USC § 2701 *et seq*. And it adopted the pen register and trap and trace statute, 18 USC § 3121 *et seq.*, governing real-time interception of "the numbers dialed or otherwise transmitted on a telephone line." (A pen register collects the "electronic or other impulses" that identify "the numbers dialed" for outgoing calls and a trap and trace device collects "the originating number" for incoming calls.) To obtain such an order, the government need merely certify that "the information likely to be obtained is relevant to an ongoing criminal investigation." 18 USC §§ 3122-23. (There is no constitutional or statutory threshold for opening a criminal investigation.) The law states that the judge "shall" approve any request signed by a prosecutor.

ECPA did not, however, extend full Title III protections to email sitting on the server of an ISP. Instead, it set up a two-tiered rule: email in "electronic storage" with a service provider for 180 days or less may be obtained only pursuant to a search warrant, which requires a finding of probable cause, but the additional protections of Title III -- limited number of crimes, high level approval, judicial supervision -- do not apply. Email in storage for more than 180 days and data stored on a "remote computing service" may be obtained with a warrant or a mere subpoena. In no case is the user entitled to contemporaneous notice. The email portions of ECPA also do not include a statutory suppression rule for government violations and do not require annual reports of how often and under what government access, which are critical for public or congressional oversight.

Mapping the Fourth Amendment onto Cyberspace

Remarkably, ECPA was the last significant update to the privacy standards of the electronic surveillance laws. Astonishing and unanticipated changes have occurred since 1986:

- the development of the Internet and the World Wide Web as mass media;
- the convergence of voice, data, video, and fax over wire, cable and wireless systems;
- the proliferation of service providers in a decentralized, competitive communications market;
- the movement of information out of people's homes or offices and onto networks controlled by third parties;
- the increasing power of hand-held computers and other mobile devices that access the Internet and data stored on networks.

As a result of these changes, personal data is moving out of the desk drawer and off of the desktop computer and out onto the Internet. Unless Congress responds, the Fourth Amendment protections would remain available only in the home when increasingly information is not stored there

Lauren B. Steinfeld
07/06/2000 12:54:47 PM

Record Type: Record

To: Joshua S. Gottheimer/WHO/EOP@EOP

cc: Peter P. Swire/OMB/EOP@EOP
Subject: Numbers using cable modems for Internet service

Public reports count approximately 2.2 million total subscribers to the Internet using cable modems. I'm am still trying to find out what share of the market this represents.

Joseph B. Trahern
07/09/2000 04:25:04 PM

Record Type: Record

To: Joshua S. Gottheimer/WHO/EOP@EOP

cc:
Subject: acknowledgements for Klink reception

note: Klink is planning on making the acknowledgments, but just to be safe;

Rep. Ron Klink (wife: Linda)
Rep. Bob Brady
Rep. Chaka Fattah
Rep. Bob Borski
Rep. Joe Hoeffel

Mayor John Street
former mayor and DNC Chairman Ed Rendell
PA Auditor General Bob Casey, Jr. (Bobby)

Technology is changing so rapidly – key is to keep our laws in synch with our progress
Great potential/ progress/ discovery also brings great responsibility, new challenges. Just last week discovered human genome – [see genome speech]. That's something that our country and our courts have responded to since our founding, and it's something we will continue to do as we evolve as a nation. Over the last 7 years, w/ the advances medicine and technology, we've done x, y, z.

Our admin has worked hard to keep up w/ our progress (in may … ea michigan commencement, medical privacy, signed eo …) … as judge brandeis said, " update our laws"

not framing

One area that's always been at the forefront of concern has been privacy (4th amendment privacy principles). Particularly true w/ laws that directly relate to our civil liberties – law enforcement (balance), and wire tapping. Historically been a 4th amendment issue, which states X. key has always been balance: between public good and civil liberties.

Original intent of forefathers

Here of course technology is always changing.
In the 18XX… the threshold for invasion privacy – protection privacy, home, diary … assume whether or not in a sphere of privacy.

Over time it has been updated:
In 1920, when first seminal case on tapping heard – olmstead. At that time, only

In 1968, … time of the case … law changed. Katz said x … Focused on phone, although there were websites at the time. Title III out of that. Email.

In 1986, … something I worked on closely … cell phones … passed x law to keep up w/ nascent web … ECPA. Forward looking at the time.
That law says:

But now – times have indeed changed again. We need to change w/ them, like our forefather did, and at other seminal moments in our history. Since 1986, x websites have been created. More than 2.2M cable modem subscribers. Then there were only 50… now over 50M. But the law still says x. It's easier today for fed officials to gain access to my grandmother's cookie recipe she sent me on aol, than a terrorists master mind plan sent on his cable modem. Cable law from 1984 says 10 days. Don't need x, y, …

We need to update our law – harmonize them. So that equal laws for electronic tapping as wire tapping. so we can strike that balance – where cable not too difficult. Email not so easy. Privacy vs. law enforcement – so if drug, child porn.

We should update our laws so they do: x, y, z

Conclusion

Shesol@aol.com
07/09/2000 10:19:32 PM

Record Type: Record

To: Joshua S. Gottheimer/WHO/EOP

cc:

Subject: Re: DRAFT--Asian Amer Advisory Video.

In a message dated 7/9/00 6:38:04 PM Eastern Daylight Time, Joshua_S._Gottheimer@who.eop.gov writes:

<< From building the transcontinental railroad
to bringing us the world?s first Pentium chip -- from public service to the
performing arts >>

I might invert this, so that the pub service/arts one comes first, just so you don't lose the thread of the "from...to..." (since the railroad/Pentium one is quite long).

Mara A. Silver
07/07/2000 12:19:27 PM

Record Type: Record

To: James A. Streett/WHO/EOP@EOP

cc:
Subject: website.0707

---------------------- Forwarded by Mara A. Silver/WHO/EOP on 07/07/2000 12:18 PM ---------------------------

Ellen E. Olcott
07/07/2000 12:00:23 PM

Record Type: Record

To: See the distribution list at the bottom of this message

cc:
Subject: EMBARGOED until 7/8 POTUS remarks in webcast

THE WHITE HOUSE

Office of the Press Secretary

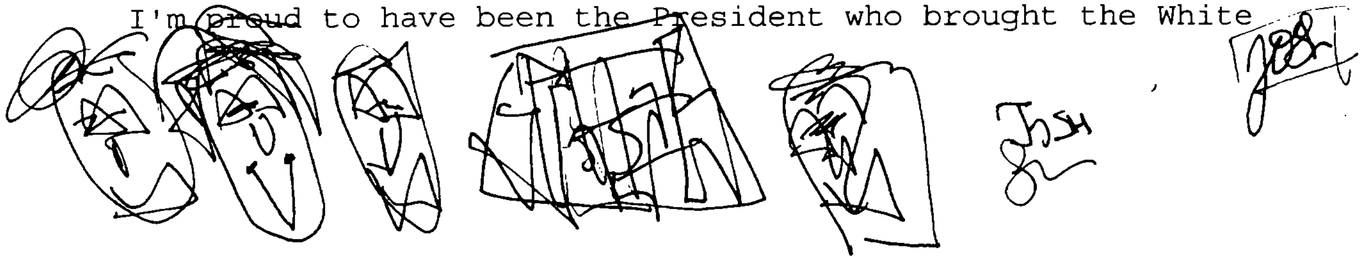
Embargoed For Release
Until 10:00 A.M. EDT
Saturday, July 8, 2000

REMARKS BY THE PRESIDENT
IN INTERNET WEBCAST

The Oval Office

THE PRESIDENT: Good morning. Earlier this week, we launched a new and improved White House website at www.whitehouse.gov. Today, I want to talk a little about the website and about our other efforts to use technology to bring government closer to the people.

I'm proud to have been the President who brought the White



House into the digital age. When I became President, there were just 50 websites on the Worldwide Web. Now, there are 17 million, and almost 50 million households on-line in the United States alone.

It was just six years ago that we launched the very first White House website. Our website now has more than 9,000 pages of information -- and that's not counting the archives. We've redesigned and updated it to keep pace with its growth and the rapid changes in technology. The new and improved White House website is another important step in our efforts to make government high-speed, high-tech and user-friendly. We're bringing information that matters into people's homes -- policy papers, the citizens' handbook, links to federal agencies.

We've also made it easier to find the features that visitors use most -- like e-mailing the White House, taking an on-line tour or finding special activities for kids. And we've made the website a permanent part of the Executive Office of the President, so that future Presidents will be able to change it to suit their needs as easily as they can change the furniture here in the Oval Office.

Under the leadership of Vice President Gore, we've used information technology to bring government closer to citizens in many ways. People are now using U.S. government websites to file their taxes, compare their Medicare options, and find good jobs. They're tapping into the latest health research, browsing the vast collections of the Library of Congress, and following along with NASA's missions in outer space.

And we're in the process of creating a single, customer-focused website, www.firstgov.gov, where Americans can find every on-line resource offered by the federal government.

But we must do more to ensure that the benefits of the information revolution flow to every American. That means working to close the digital divide, to put computers in every classroom, to train our teachers to make the most of them. We must also pay attention to the issues of computer security and the privacy of our records on computers, so that the newest technology doesn't undermine our oldest values.

Eighty-one years ago this week, Woodrow Wilson became the very first President to communicate by radio. On his way home from Europe, President Wilson used the radio, after several unsuccessful efforts, to call the then-young Franklin Roosevelt, who was his Assistant Secretary of the Navy back in Washington. It wasn't immediately clear how this new technology would be used, or that in just 15 years Roosevelt, as President, would be making radio broadcasts that 80 percent of our nation would hear. But it was clear that a new door to the future had opened.

We're at just such a moment again today, and the new White House website is just one small step toward bringing government more fully into the Information Age. We have barely begun to understand how information technology will change our lives. But those of us in government have a responsibility to use these new tools to expand the reach of democracy and give more people a chance to live their dreams.

I'll see you on line at whitehouse.gov, and thanks for logging on.

END

Message Sent To: ____

THE WHITE HOUSE
WASHINGTON

Ideas · ECBA

what law ~~etc~~ requires — set ECBA

email

strict certain areas

ECBA — ~~cable rules~~

electronic
wire
tap —
communication

✓ Cable statute — 1984

June 27, 2000 Rob J →

Initial draft for Podesta National Press Club speech on Cyber-Security

[Add introductory paragraphs -- glad to be here today, etc.]

Let me begin today with the text of the Fourth Amendment to the United States Constitution, ratified 213 years ago:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated"

As you can see, the text of 4th Amendment protects not only your "person" and "house" but also the right of the people to be secure in their "papers and effects." In 1787 [or: At the time of the Framers], a person's most important "papers and effects" were almost undoubtedly in their home or place of business. Our "papers and effects" were thus protected by the requirement of a warrant before the state could enter and search.

Today, as Americans spend more and more time in cyberspace, that is less and less true. Consider the extent to which our e-mails already contain so much of our sensitive thoughts and information. Shouldn't these e-mails count as "papers and effects?" Yet these e-mails are held outside of our houses on computer servers.

Looking ahead, even more of our "papers and effects" may be kept outside of the home. Consider the rise of "ASPs" or application service providers. [We have a press quote from April: "This segment of the IT industry has become one of the fastest growing markets."] Under this approach, our word processing software and files would also be kept on servers, accessible to us as we travel through our busy lives, but also possibly accessible to the government or others outside of the home.

Will the courts automatically protect these "papers and effects" under the 4th Amendment? The answer seems to be no. Under the 4th Amendment, the Supreme Court has said that individuals consent to release of their information when they send data to their bank or e-mail provider. The government can constitutionally then ask the bank or e-mail provider for that data, without the need for legal process. Only if there is a statute in place, such as the Right to Financial Privacy Act for banks, are there legal requirements before the government can seek the information.

As a matter of constitutional doctrine, the 4th Amendment thus may not protect these "papers and effects." But as a matter of public policy -- of the choices we make as a democracy -- shouldn't people's most private "papers and effects" be given significant legal protection? The genius of the 4th Amendment is that it protects Americans' homes against unreasonable searches. But reasonable searches -- those done with the right legal protections -- are allowed.

My topic for today, then, is how to provide the right legal protections for our "papers and

This is an area where the Govt and the

effects" in cyberspace. When so much of our sensitive personal information is kept outside of our home, what should the rules be for government access to that data? How do we give continuing vitality to 4th Amendment values when the facts have changed, and "papers and effects" are kept outside of the home?

In discussing cyber-security and 4th Amendment values, my talk today is part of the broader Administration efforts to construct a framework for building trust and security in cyberspace. Today I am focusing on law enforcement authorities and how they should be updated to address the new challenges and opportunities of the Internet. The broader framework, however, includes the following major pieces:

- *Private sector leadership.* As emphasized at the President's Cyber Security Summit with industry leaders in February, most computers and networks that we rely upon are owned and operated by the private sector. The private sector ~~thus has a responsibility to lead~~ in implementation of computer ~~and network~~ security. The more the public and industry do ~~on their own~~, the less need we will have for law enforcement to handle problems through criminal enforcement.

- *Government as a model citizen.* A key role for the federal government is to be a model for information security and ~~privacy practices~~, and for building trust in the Digital Society. We have taken many steps to act as such a model, such as my report on how agencies have responded to distributed denial of service attacks and guidance from the Director of OMB to assure that appropriate security measures are included as part of the funding of all government computer systems.

- *Public-private partnership.* The federal government will work in partnership with the private sector to build security and trust in online activities. The National Plan for Information Systems Protection was issued in January, and we have a number of efforts underway to build ~~this partnership.~~

- *Preserve fundamental American values such as privacy and civil liberties.* Creating security and trust on the Internet must be done with dedication to longstanding values including: protection of privacy and civil liberties; improving the quality of life for all Americans, such as through the promotion of electronic commerce and elimination of the digital divide; and furthering of the educational ~~and free speech~~ potential of the Internet.

Turning more specifically to the law enforcement context, the three themes I wish to stress today are *updating, harmonization, and balance.* Historic, recent changes in technology mean that we must *update* the rules for law ~~enforcement~~ access to electronic communications. The basic rules for law enforcement access to telephone calls were enacted in 1968. The last major updating of these sorts of rules came in the Electronic Communications Privacy Act (ECPA) of 1986 -- years before most Americans had even heard of the Internet.

Protecting Electronic Messaging: A Guide To The Electronic Communications Privacy Act Of 1986

By
John Podesta & Michael Sher
Podesta Associates

EMA

Published By The Electronic Mail Association

Contents

Foreword

As the Senate sponsor of the Electronic Communications Privacy Act of 1986 (ECPA), 18 USC 2510 et seq., I was pleased to learn that the Electronic Mail Association planned to publish a guide to the law—a law that is vital to both the consumers and providers of electronic information.

The Electronic Communications Privacy Act helps ensure the privacy of communications transmitted by the most advanced technology, including electronic mail, on-line computer databases, remote computing systems and sophisticated telecommunications systems. In 1986, when ECPA was enacted, the need for the law was apparent. At that time, phone calls made over our nation's telephone lines were protected against interception and eavesdropping, but electronic communications sent over the very same telephone lines were afforded no such protection. The privacy of our nation's communications was governed by a law (Title III of the Omnibus Crime Control and Safe Streets Act of 1968) that was hopelessly out of date. That law was passed when Congress could barely contemplate the new forms of telecommunications and computer technology that would emerge in the last quarter of the 20th century.

Today, Americans have at their fingertips a broad array of telecommunications and computer technology, including electronic mail, voice mail, electronic bulletin boards, interactive video, and on-line computer access to some of the world's most valuable databases.

That is why my colleagues in Congress, including Senator Charles Mathias of Maryland, and Congressmen Robert Kastenmeier of Wisconsin and Carlos Moorhead of California, worked for two years in the spirit of bipartisan cooperation to fashion a new law to protect the privacy of communications into the 21st century.

The Electronic Communications Privacy Act ensures the integrity of electronic communications by making it a federal crime to intercept and disclose electronic communications, in much the same manner that the wiretap statute prohibits the interceptions of telephone calls. The law also makes it a crime to gain access, without permission, to electronic communications in storage.

ECPA not only protects American consumers, but is vital to the continued growth of the electronic communications and high technology industries in the United States. The law assures individual Americans and American businesses that their communications will remain confidential and so encourages consumers to make use of these exciting new technologies. ECPA also provides law enforcement officials with the tools to protect our nation's electronic communications networks, computer systems and databases from high-tech criminals. For all these reasons, ECPA enjoyed wide support among industry and consumer groups, privacy advocates such as the Individual Rights and Responsibilities Section of the American Bar Association and the American Civil Liberties Union, and the Department of Justice.

The Electronic Mail Association (EMA) played an important role in the development of ECPA. Mike Cavanagh, executive director of EMA, and Phil Walker, vice president of Sprint International, and one of the founding members of EMA, were able negotiators who not only represented their industry well, but helped provide a broader vision of the need to safeguard individual privacy, as well as technology, in an era of rapid change and innovation. It is especially appropriate that EMA has published this important new guide to the Electronic Communications Privacy Act. Congress intended that ECPA help nurture industries such as the electronic mail industry. It is therefore important that members of the industry understand their rights and responsibilities under that law.

Finally, I want to recognize the authors of this guide. John Podesta served me loyally as my chief counsel on the Senate Judiciary Committee for more than seven years. During much of 1985 and 1986 he managed the effort to enact ECPA into law. John directed the negotiations among interested Members of Congress and concerned parties and drafted the bill that ultimately became law. For these reasons, alone, John is singularly well-qualified to explain the law.

I also had the pleasure of working with Michael Sher, who co-authored this guide with John. Michael served as my legislative assistant for economic issues between 1985 and 1989 and during that time worked closely with representatives of the growing high technology industry in my state of Vermont.

Senator Patrick Leahy
United States Senate

Introductior

Less than a decade ago, electronic mail technology was used by only a few hundred thousand Americans, many of whom were advanced research scientists. Today, over ten million Americans use messaging technology, and the typical profile might be a salesperson who takes her laptop computer on the road to meet with prospects, or the designer who needs to gain approvals from appropriate corporate management before his new product can go into production.

During the 1980s, a range of new electronic communications technologies gained wide acceptance from the public, and while these new technologies represented great steps forward, they also inevitably raised public policy and legal issues that required serious attention by appropriate government institutions. Indeed, in this latter part of the 20th century, dramatic advances in all aspects of technology have presented a distinct challenge to our legal entities.

In the case of electronic communications privacy, we perhaps have a blueprint of the kind of responsible action that can be taken to update laws using centuries-old principles as the foundation for legislative language that addresses leading-edge technology. The Electronic Communications Privacy Act of 1986 grew out of an effort by leading Congressional policymakers, their talented staffs, industry, privacy watch-dogs like the American Civil Liberties Union, and the Justice Department to resolv "high tech" communications issues. The Electronic Mail Association was proud to play a central role in providing lawmakers with industry data and recommendations during the drafting process and in leading lobbying efforts in support of passage of the bill.

EMA is now very pleased to make available this detailed guide to the law with essential information from the Justice Department relating to its interpretations of key aspects of the legislation. After new laws are enacted, it traditionally takes some time before various memoranda are issued relating to these interpretations, but we feel a guide like this one can now be issued, with the understanding that clarifications, amendments, court rulings, etc., can certainly be expected. This guide is deliberately being issued in a binder format, and EMA will be committed to updates when appropriate.

As executive director of the association, it was my great pleasure to work with the guide's authors, John Podesta and Michael Sher. John served as chief counsel of the Senate subcommittee responsible for ECPA and is currently a partner in the consulting firm he founded with his brother, Podesta Associates. John's service on the Senate Judiciary and Agriculture committee staffs made him one of the most respected and well-liked key staff aides on Capitol Hill for many years. Michael Sher, his associate at Podesta Associates, brought years of Congressional staff experience and particular expertise in legal issues relating to wiretap laws and ECPA to thisproject. We also war to thank Phil Walker, vice president at Sprint International, for his contributions to th guide. Phil, who served as chairman of EMA during the Congressional deliberations of ECPA, devoted literally countless hours to passage of ECPA. His extraordinary telecommunications regulatory background was demonstrated again and again during the bill's successful march to passage.

While ECPA has provided traditional legal protections against outside intrusion to users of data communications, it is important to note that the subject of workplace privacy is receiving new scrutiny today in various quarters. Monitoring of telephone calls, inside mail, and electronic mail has been challenged by employees who have felt victimized by such practices.

Although privacy in the workplace has been ill-defined in the past, it would seem to make good common sense for organizations to review what policies, if any, they maintain with respect to records management and/or information dissemination, because Federal laws governing outside interception (postal privacy laws, the wiretap act, and ECPA) generally do not apply in intra-corporate situations. Organizations should also carefully scrutinize applicable state workplace privacy laws.

The electronic mail industry, like others involved in communications and information storage and retrieval, can perform a valuable service by addressing the myriad of issues that arise when one examines workplace privacy.

A final note should be made in this introduction relating to the detail that will be found in this guide. To be sure, our direction to the report's authors was to provide us with a comprehensive overview of the key provisions of ECPA. This document represents the kind of guide that can be referred to in any of a number of circumstances. The basic principles of ECPA are clear and can be understood by all, just as mail privacy guidelines and wiretap laws are simple in concept.

For attorneys responsible for analyzing the validity of requests presented to them by a law enforcement officer, we hope that the specific information on "when the government comes calling" will be helpful. Likewise, we hope that operations staff seeking clarification of backup storage issues delineated in ECPA will find the guide informative, as will any individual unaware of ECPA who might think that unauthorized access to someone's electronic mailbox is a legally ambiguous act.

Michael F. Cavanagh
Executive Director
Electronic Mail Association

Preface

Configuration Of Electronic Mail Systems Is Key To Rights And Responsibilities

A. Purpose

The Electronic Communications Privacy Act has two essential purposes: 1) to protect **all** electronic communications systems, including purely internal electronic mail systems and public systems, from outside intruders; and 2) to protect the privacy of certain messages sent over public service electronic mail systems just as the privacy of telephone calls over public telephone systems is protected.

First, the Electronic Communications Privacy Act protects all electronic mail systems, regardless of whether they are purely internal or public systems, from outside hackers, intruders and other unauthorized users who break into systems, steal or manipulate information, or cause damage to the system. The law creates a deterrent against outside intruders by providing prison terms and criminal fines for offenders who illegally access or exceed their authorized access to an electronic communications system.

Second, the privacy provisions of the new law—the rules concerning the disclosure of electronic mail messages—afford markedly different benefits and impose very different responsibilities depending on the configuration of an electronic mail system. Specifically, the law treats purely internal electronic mail systems differently from those public service systems operated for use by outside businesses, the general public, or to forward messages.

The privacy provisions of the new law are applicable only to a person or entity providing an electronic communication service to the public.[1] Operators of purely internal systems need generally only be concerned with the protections the new law provides against outside intruders and electronic wiretappers. Purely internal systems are not subject to the privacy provisions of ECPA, and the new law does not impose restrictions on the disclosure of messages sent on purely internal systems, including electronic mail messages sent by employees of a firm that uses a purely internal electronic mail system.

In large part, the privacy provisions of ECPA seek to protect the privacy of communications made on large **public service** electronic mail systems. These **public service** electronic mail firms operate much like public telephone utilities. An outside individual or company subscribes to the public service and can send messages to other individuals and firms via the service.

Public service electronic mail firms are experiencing significant growth and are becoming an important part of the electronic mail industry. ECPA has helped public service firms grow by protecting the privacy of messages sent over these systems and thereby providing businesses and individuals confidence that their messages will remain secure. The law protects the privacy of messages by creating a deterrent against illegal disclosure: just as telephone customers can sue the phone company for illegally listening to phone calls, injured parties can bring suit in the event that a public service electronic mail firm discloses a message without authorization or pursuant to the exceptions set out in the law.

This preface will help electronic mail systems executives and operators determine whether their system is subject to the privacy provisions of ECPA. The preface will explain the distinctions between private and public electronic mail systems, and hopefully will aid the reader in understanding the rules explained in the following chapters concerning the different kinds of electronic mail systems.

B. Classifications Of Electronic Mail Systems

1. Purely Internal Systems

By far, the greatest number of electronic mail systems are purely internal and are **not** subject to the same stringent rules concerning the disclosure of messages imposed upon companies that offer electronic mail services to other businesses or to the public.

There are two types of internal electronic mail systems. First, some companies and organizations acquire their own on-site computer systems with an electronic mail component. Second, many companies without their own on-site electronic mail systems contract with large public service electronic mail firms to use portions of the larger company's electronic communications system to provide **solely** internal messaging. Both of these types of electronic mail systems are considered internal, and messages sent over them are not subject to the restrictions on disclosing and monitoring messages.

Since internal messages are not protected by the privacy provisions of ECPA, and are treated much like workplace-generated paper memos, they generally may be read by authorized supervisors, co-workers and systems managers without violating ECPA. While federal law may not bar authorized personnel from accessing another employee's messages, and indeed, business necessities may require it, managers, as a matter of sound business practice, should consider informing the users of an internal electronic mail system of their rights and responsibilities with regard to the confidentiality of messages sent on the system. Most system managers may want to deal with these issues through normal system training.

2. Public Electronic Mail Systems

A number of major firms in the electronic mail industry offer electronic mail services to other businesses and to the public. These firms also forward messages from one electronic mail system to another. In most respects, ECPA treats these public service electronic mail providers just as telephone companies are treated under the wiretap statute. Public service electronic mail firms may only turn over messages to law enforcement officials if an appropriate warrant, court order or subpoena is presented. Furthermore, these firms may expose themselves to litigation if they improperly disclose or intercept electronic mail messages.

3. Internal Systems That Allow Outside Users

Two situations may arise when a firm with a purely internal messaging system opens up the system to permit outside individuals to send and receive messages.

First, some businesses with internal messaging systems may permit individuals outside the business to communicate **with the firm** by sending and receiving messages on the firm's internal system. For instance, a manufacturer with an internal electronic mail system may permit suppliers to use the electronic mail system to process orders and invoices. Messages sent on this internal system by the outside supplier may be disclosed by the manufacturer/system operator under ECPA. ECPA permits either the sender or recipient to disclose the contents of a message just as a sender or recipient of first-class mail may make numerous copies of, and distribute, a letter he or she sent or received. Under this example, the manufacturer would be considered the recipient of any message sent via the internal mail system by the outside supplier and therefore could disclose the message. The same would be true of any message the manufacturer sends to the supplier via the system.

A second, and more difficult case arises where a system permits an outsider to use a company's internal mail system to send a message to another outsider. For instance, in our example, the manufacturer may allow numerous outside suppliers to use its internal electronic mail system to do business with the manufacturer. As long as the messages are sent to and received by the manufacturer that operates the system, the system remains internal and none of the rules against disclosure applies. However, if the system's operator permits one outside supplier to send messages via the internal system to another outside supplier, the situation is less certain and may begin to approximate a public service electronic mail service.

While there is no guidance provided in the legislative history of ECPA and there has been no litigation in this area, a reasonable interpretation of the law would suggest that messages sent by outsiders to outsiders via an internal system would not be subject to the rules against disclosure, as long as the message traffic is incidental and the electronic mail system provider does not charge for messaging. On the other hand, if traffic between the outsiders increases substantially or if the electronic mail system operator charges for messages between outsiders, the system runs the risk of being considered a public service electronic mail provider and may be subject to the rules against disclosure.

4. Hybrid Electronic Mail Systems

A special situation arises for **a handful of large public service electronic mail firms** that also offer private, in-house electronic mail systems for their employees. In some cases, these internal and public electronic mail systems are connected, allowing an employee on the internal system to send a message from the internal system to a party outside the company over the public electronic mail system. Chapter 1 discusses these hybrid systems in greater detail and suggests that once a message (even a message originated on a purely internal system) is sent over a public system, the message may be subject to ECPA's rules against disclosure.

1. 18 U.S.C.A. sec. 2702(a) (West Supp. 1988).

service to federal government agencies, are subject to strict rules concerning the disclosure of electronic mail messages in the transmission stage.[7] Failure to comply with these rules can expose a firm and its employees to civil liability.

Subject to the very logical exceptions discussed below, electronic mail firms offering service to the public may not **intentionally** disclose the contents of any message while in transmission to anyone other than the intended recipient of the message or his agent.[8] For example, inadvertent disclosure of electronic mail messages to a mistaken recipient are not punishable under this section. But where a firm makes it a conscious objective to disclose electronic mail messages to parties other than the intended recipient, the firm opens itself up to criminal and civil liability.[9]

The rule against intentional disclosure clearly applies only to systems offered to the public. Therefore, if a manager of a purely internal electronic mail system discloses to a company executive a suspicious message intended for another employee, neither the firm nor the system's manager would be criminally or civilly liable under ECPA. While no civil liability may arise under ECPA, a recent case filed in California challenges the right of employees to read electronic mail messages under California state privacy and employment law. (*Shoars v. Epson America Inc.*)

3. *Special Rules For Firms With Internal And Public Components*

The situation is less certain for those companies that operate hybrid systems with both internal messaging and public electronic mail services. Currently, these rules only apply to a handful of large public electronic mail firms which also have internal systems for their employees.

A narrow reading of the law suggests that an electronic mail firm offering service to the public may not intentionally disclose the contents of a message while in transmission on **that service.**[10] Therefore, this way of reading the new law would suggest that where an electronic mail firm offers separate internal and public services, the firm could disclose messages sent on the internal service, but would be criminally and civilly liable if it discloses messages on a public service.

In some cases, however, an electronic mail firm may have an internal messaging system that also allows employees to access the public system and send messages originated on the in-house system. Although the legislative history and Justice Department guidelines offer little guidance on the subject, a reasonable reading of the law suggests that an electronic mail firm may disclose a message that originated on its in-house messaging system and was sent out via its public service. The public service system would be considered the legal owner and thus the originator of the message under ECPA because it maintained the internal messaging systems for its own business use.[11]

While there have been no court interpretations of this provision of the new Act to provide guidance to electronic mail firms, cases are beginning to arise in which claims of confidentiality are being made with respect to hybrid systems. For example, a recent controversy has erupted in Colorado Springs, Co., over the disclosure to the city's mayor of electronic messages between city council members. While the system is owned and operated by the city, it was designed to be accessible by the public. Firms should be cautious about **intentionally** disclosing messages sent on a hybrid, public/private electronic mail system. These are uncharted legal waters and firms should be careful about exposing themselves to criminal and civil actions.

C. The Exceptions

1. Exceptions Which Permit Interception Or Disclosure

Congress recognized that there are cases in which an electronic communication must be intentionally intercepted or disclosed, for instance, in those situations where one electronic mail firm must pass on a message to another firm for forwarding. This exception is similar to the exception in the wiretap statute which permits local telephon companies to forward calls to long distance carriers. Therefore, while it is generally a felony to intercept an electronic mail message, or disclose or use an electronic mail message which has been intercepted, the following exceptions apply.

a. *It is not illegal to intercept an electronic communication made through an electronic bulletin board or other communications system that is configured so that it is readily accessible to the public.*[12] However, communications sent over the private element of a computer system that features a separate electronic bulletin board element continue to be protected against interception.

b. *It is not illegal for an employee or agent of an electronic mail firm to intercept, disclose or use an electronic mail message in the normal course of business, when engaged in activities necessary to providing services, or to protect the rights or property of an electronic mail provider.*[13] Congress recognized that electronic communications providers may have to monitor a stream of transmissions in order to properly route, terminate or manage individual messages. This type of monitoring is not prohibited because it does not infringe on the privacy of either the sender or recipient. On the other hand, phone companies are not permitted to monitor telephone conversations in order to route them, nor is the Postal Service permitted to read letters in order to dispatch them.[14]

c. *It is not illegal to intercept an electronic communication, including an electronic mail message that is harmfully interfering with an operating station or consumer* *electronic equipment, in order to identify the source of the interference.* [15] It is important to note that interception is only permitted to identify the source of harmful interference.[16] A literal reading of the law would suggest that once an electronic mail firm has determined the source of the interference, it must stop intercepting the messages.

d. *It is not illegal for an electronic mail firm to record the initiation and/or completion of an electronic message.*[17] The statute permits electronic mail firms to record the duration of messages just as the phone company is permitted to record the length of calls for billing purposes and to protect the company and its customers from fraud and abuse.[18] Electronic mail firms may use pen registers and trap and trace devices for billing purposes or to track down individuals abusing the system.[19] See the chapter on pen registers and trap and trace devices for greater detail.

e. *It is not illegal for the sender or recipient of a message to intercept, disclose or use an electronic mail message.*[20] For example, this exception allows the sender of a message to intercept a message before it reaches its intended recipient in order to make changes or even to prevent the recipient from receiving an unintended message. In addition, this provision takes the logical step of protecting the right of the recipient of an electronic mail message to "intercept" or receive a message and then "disclose" or share that message with other electronic mail users. For example, many times an electronic mail customer will receive a message and want to forward it to other electronic mail users. This type of activity is not illegal under ECPA.

f. *It is also not illegal for a third party to intercept, disclose or use the message when either the sender or recipient gives his or her permission.*[21] For example, if a reporter asks to monitor an electronic mail message sent by Party A to Party B and either party gives his or her permission, the reporter could intercept the message, and disclose and use it in a newspaper article. This exception does not apply, however, when a message is intercepted for purposes of committing another crime (such as blackmail) or act which causes tortious injury to another (for example, if the hypothetical reporter used the intercepted message to commit libel).[22]

2. Special Exceptions For Public Electronic Mail Systems

Just as Congress realized that there must be exceptions to the rules against intentionally intercepting electronic messages (e.g., so that a sender can make corrections in a message), Congress included exceptions to the rule generally prohibiting electronic mail firms from disclosing the contents of electronic mail messages while in transmission. While it is generally illegal for an electronic mail firm that offers service to the public to provide a message to anyone other than the person whom the sender intended to receive the message, ECPA provides the following practical exceptions:

a. *It is not illegal for an electronic mail firm to disclose the contents of a message to third parties with the consent of either the sender or the intended recipient.*[23] For example, a client who sends a message via an electronic mail service may ask the electronic mail service to provide an additional copy of a message to a third party without the consent of the original intended recipient. All that is needed is the permission of the sender. This rule is similar to the one-party consent exception to the wiretap statute which allows one party to ask the telephone company to connect a third party to a phone call.[24]

b. *It is not illegal for an electronic mail firm to disclose the contents of a message to individuals or other firms involved in forwarding the message.*[25] For example, if a message is being sent through an electronic mail network involving two or more electronic mail firms, the electronic mail firm responsible for sending the message may legally pass the message on to a second firm for routing and delivery. The same is the case under the wiretap statute, which permits local phone companies to forward messages to long distance carriers. This section of ECPA was included specifically to exempt communications intermediaries from the ban on disclosing the contents of messages.[26]

c. *An electronic mail service may disclose the contents of a message to law enforce ment officials when the contents were obtained inadvertently and appear to concern the commission of a crime.*[27] This exception only applies when an electronic mail provider obtains the information inadvertently and not when the "provider purposefully sets out to monitor [messages] to ascertain whether criminal activity has occurred."[28] Congress envisioned this circumstance as being exceptional.[29] For example, if an employee of an electronic mail firm is monitoring a stream of transmissions and accidentally happens to see a message relating to a narcotics transaction, the employee and employer may disclose the contents of that message to the police.

d. *Finally, the rule against disclosing the contents of electronic mail in transmission does not apply to firms that operate purely private, internal messaging systems.* Rather, the restrictions only apply to firms providing "an electronic communication service to the public."[30]

D. The Penalties (Criminal And Civil)

1. *Criminal Penalties For Interception*

Illegally intercepting electronic mail, or illegally disclosing or using illegally intercepted electronic mail, is a federal felony punishable by up to five years in prison and/or a fine of up to $250,000 for individuals and $500,000 for organizations.[32]

2. Civil Action For Illegal Interception

Just as an individual whose phone has been tapped illegally may sue the wiretapper under the wiretap statute, any person whose electronic mail is illegally intercepted, disclosed or used may sue the person or organization that violated the law for damages in a civil lawsuit.[33] A plaintiff may bring a civil action regardless of whether the defendant has been the subject of a criminal prosecution. But in the absence of a criminal prosecution, the burden is on the plaintiff to demonstrate that there has been a violation of the law.[34]

Both actual and punitive damages are available as remedies. In addition, an electronic mail firm can obtain preliminary and permanent injunctions to stop illegal interceptions.[35] Reasonable attorney's fees and litigation costs may also be awarded.[36] A court may calculate damages by awarding statutory damages of $100 per day or $10,000, or actual damages, whichever is greater. If actual damages are awarded, a plaintiff can also receive any profits derived by the violator from any illegal activities.[37]

3. Injunctions And Civil Fines For Illegal Interception

In addition to the provisions that permit an electronic mail firm to go to court to obtain an injunction, whenever it appears that a person is committing a felony or is about to commit a felony under ECPA (e.g., illegally intercepting, disclosing or using electronic mail), the U.S. Attorney General is given authority to bring a civil suit to enjoin the illegal activity.[38] The violation must present the threat of a continuing and substantial injury to the United States or to any person or class seeking protection.[39] This provision is similar to the federal statute providing for injunctions against fraud.[40] The ability to obtain injunctions and temporary restraining orders in a separate civil case is important because a prolonged criminal investigation and prosecution would otherwise permit illegal activities to continue while the case works its way through the criminal system.

4. Civil Suit Against Electronic Mail Providers For Disclosing Contents Of Messages

Just as an individual who illegally intercepts electronic mail is subject to a civil suit for damages, so, too, are electronic mail firms which illegally disclose the contents of electronic mail while in transmission. Firms violating the law may be liable for actual and punitive damages, along with attorneys fees and litigation costs.[41] As is the case with illegal interceptions, firms that illegally disclose electronic mail messages in transmission may be liable for damages for each violation equaling the actual damages suffered by the plaintiff, plus any profits made by the firm from disclosing the message, or statutory damages of up to $10,000, whichever is greater.[42]

5. *Exclusivity Of Remedies*

The remedies and criminal sanctions for the interception of electronic communications are the only remedies and sanctions available, except in the case of constitutional violations. Remedies for constitutional violations (e.g., violations of the Fourth Amendment by law enforcement officials to be remedied by invoking the exclusionary rule), however, only apply to the government. Therefore, a customer suing an electronic mail firm for disclosing a message while in transmission, must sue under the new rules set out by ECPA, which also establishes defenses for electronic mail firms that acted in good faith and complied with the statute.[43]

E. The Defenses In Criminal And Civil Actions

In the event that an electronic mail firm is sued for disclosing the contents of a message while in transmission, ECPA sets out a number of defenses to ensure that a firm will not be held liable for properly cooperating with law enforcement officials or for following the exceptions in the law to the rule against disclosure. (Chapter 2 describes in detail the procedures a firm should follow in cooperating with law enforcement officials who want to intercept electronic mail transmissions.)

An electronic mail firm may defend itself in any criminal action or civil suit that challenges the disclosure of a message by offering one of the following complete defenses:

• The disclosure was made in good faith reliance on a court order, warrant or subpoena.[44] Thus, an electronic mail provider that has received a court order would be entitled to a dismissal of a civil suit if it acted within the scope of the court order.[45] (See next chapter for greater detail.)

• The disclosure was made in good faith reliance on a statutory or legislative authorization.[46]

• The disclosure was made in good faith reliance on a written certification by a specially authorized law enforcement officer that an emergency situation exists which made it impossible to obtain a court order before the fact.[47] (See next chapter for greater detail.)

• The electronic mail provider disclosed the information based on a good faith determination that the exceptions to the general rule against disclosure (e.g., the exception for disclosing the contents of a message to another firm for forwarding) apply.[48]

Finally, ECPA created a two-year statute of limitations for bringing a civil suit. Any civil action must be commenced no later than two years after the party bringing the suit has a reasonable opportunity to discover the violation.[49]

1. 18 U.S.C.A. sec. 2511(1) (West Supp. 1988).
2. 18 U.S.C.A. sec. 2511(1)(b) (West Supp. 1988).
3. 18 U.S.C.A. sec. 2511(1)(d) (West Supp. 1988).
4. S. Rep. No. 541, 99th Cong., 2nd Sess., 23 (1986).
5. Id. at 23, 24.
6. Id. at 24.
7. S. Rep. No. 541, 99th Cong., 2nd Sess., 25 (1986).
8. 18 U.S.C.A. sec. 2511(3)(a) (West Supp. 1988).
9. S. Rep. No. 541, 99th Cong., 2nd Sess., 23, 24. (1986).
10. 18 U.S.C.A. sec. 2511(3)(a) (West Supp. 1988).
11. 18 U.S.C.A. sec. 2511(2)(d) (West Supp. 1988).
12. 18 U.S.C.A. sec. 2511(2)(g)(1) (West Supp. 1988).
13. 18 U.S.C.A. sec. 2511(2)(a)(1) (West Supp. 1988).
14. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 47 (1986).
15. 18 U.S.C.A. sec. 2511(2)(g)(iv) (West Supp. 1988).
16. S. Rep. No. 541, 99th Cong., 2nd Sess., 19 (1986).
17. 18 U.S.C.A. sec. 2511(2)(h)(ii) (West Supp. 1988).
18. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 46 (1986).
19. 18 U.S.C.A. sec. 2511(2)(h)(i) (West Supp. 1988).
20. 18 U.S.C.A. sec. 2511(2)(c) (West Supp. 1988).
21. 18 U.S.C.A. sec. 2511(2)(c) (West Supp. 1988).

22. 18 U.S.C.A. sec. 2511(2)(d) (West Supp. 1988); S. Rep. No. 541, 99th Cong., 2nd Sess., 17, 18 (1986).

23. 18 U.S.C.A. sec. 2511(3)(b)(2) (West Supp. 1988).

24. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 49 (1986).

25. 18 U.S.C.A. sec. 2511(3)(b)(iii) (West Supp. 1988).

26. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 49 (1986).

27. 18 U.S.C.A. sec. 2511(3)(b)(iv) (West Supp. 1988).

28. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 50 (1986).

29. S. Rep. No. 541, 99th Cong., 2nd Sess., 38 (1986).

30. 18 U.S.C.A. sec. 2511(3)(a) (West Supp. 1988).

31. 18 U.S.C.A. sec. 2511(4)(a) (West Supp. 1988).

32. S. Rep. No. 541, 99th Cong., 2nd Sess., 21 (1986).

33. 18 U.S.C.A. sec. 2520(a) (West Supp. 1988).

34. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 50 (1986).

35. 18 U.S.C.A. sec. 2520(b)(1)(2) (West Supp. 1988).

36. 18 U.S.C.A. sec. 2520(b)(3) (West Supp. 1988).

37. 18 U.S.C.A. sec. 2520(2) (West Supp. 1988).

38. 18 U.S.C.A. sec. 2521 (West Supp. 1988).

39. Id, and see William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All States Attorneys and Strike Force Chiefs, December 15, 1986, 13.

40. See the Comprehensive Crime Control Act of 1984, Pub. L. 98-473; H. R. Rep. No. 647, 99th Cong., 2nd Sess., 61 (1986).

41. 18 U.S.C.A. sec. 2520(b)(1),(b)(2),(b)(3) (West Supp. 1988).

42. 18 U.S.C.A. sec. 2520(2) (West Supp. 1988). But, 18 U.S.C. 2511(3)(a) makes it unlawful for an electronic communications firm that offers service to the public to divulge the contents of communications. But the only criminal penalties are set out in Section (4)(a) which establishes a five-year prison term limited to violations of subsection (1) of 18 U.S.C. sec. 2511 which is the general interception prohibition. There do not appear to be any criminal sanctions for unlawful disclosure by an EMail firm of messages in transmission.

43. 18 U.S.C.A. sec. 2518(10)(c) (West Supp. 1988).

44. 18 U.S.C.A. sec. 2520(2)(d)(1) (West Supp. 1988).

45. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 50 (1986).

46. Id.

47. 18 U.S.C.A. sec. 2520(d)(2) (West Supp. 1988).

48. 18 U.S.C.A. sec. 2520(d)(3) (West Supp. 1988).

49. 18 U.S.C.A. sec. 2520(e) (West Supp. 1988).

Chapter 1

Protecting Electronic Mail In Transmission

A. Purpose

Title I of the Electronic Communications Privacy Act (ECPA) has two purposes: 1) to protect electronic communications, including electronic mail, from illegal interception by unauthorized third parties; and 2) to regulate when electronic communications firms may divulge the contents of communications while messages are being transmitted. Although this title protects electronic mail firms from electronic wiretappers and hackers, this section of the law also establishes significant responsibilities on the part of electronic mail firms that offer service to the public— responsibilities similar to those imposed on telephone companies of all sizes. Failure to meet these responsibilities, including protecting the privacy of your customers' electronic mail, can carry federal prison terms and heavy fines. Therefore, it is important that electronic mail firm executives and employees become familiar not only with the new protections afforded by this section of the law, but also with the responsibilities and liabilities imposed.

Firms with purely internal electronic mail systems are not subject to the same tough standards and criminal penalties as are electronic mail firms that offer service to the public. Nonetheless, it is important for executives who currently have responsibility for purely internal systems to become familiar with the rules for public systems in the event that a firm decides to open all or part of its system to the public.

7.

53047

In general, ECPA protects electronic communications from illegal interception by extending the federal criminal sanctions that apply to telephone wiretapping to electronic communications, such as electronic mail. Just as it has been a federal crime to intercept telephone conversations since enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, ECPA makes it a federal crime to intercept electronic mail, data transmissions and other electronic communications. These provisions not only protect the privacy of users of services such as electronic mail, but also provide the electronic mail industry with a means of safeguarding its systems and providing clients with a secure, efficient and attractive means of communications.

The Electronic Communications Privacy Act also regulates when electronic mail firms may divulge the contents of electronic mail in transmission, generally to ensure that only the intended recipient of a message will be able to read the message. The law does, however, provide practical exceptions to the rule against disclosing the contents of an electronic mail message to allow electronic mail firms to process and forward messages, which sometimes requires monitoring the flow of messages and passing messages on to other services. As has always been the case with telephone companies, failure to comply with the rules concerning the disclosure of customers' communications while in transmission can make an electronic mail firm liable for significant civil damages.

B. The Standards

1. Protecting Electronic Mail Systems From Illegal Eavesdropping

The Electronic Communications Privacy Act affords protection to electronic mail while it is being transmitted similar to the protection provided to telephone calls by the federal wiretap statute. This section was intended to protect electronic communications systems from individuals with criminal intent who attempt to intercept financial information and data transmissions, as well as to protect systems from eavesdroppers who simply want to read others' electronic mail. While this prohibition generally applies to outside hackers, it may in certain circumstances apply to employees of an electronic mail firm who illegally intercept electronic communications.

ECPA makes it a federal felony to **intentionally intercept**, attempt to intercept or hire someone to intercept an electronic communication in transmission.[1] It is further a federal felony to **intentionally disclose** or attempt to disclose any electronic mail communication when the person making the disclosure **knew or had reason to know** that the information was obtained by an illegal interception.[2] Finally, it is a federa' felony to **intentionally use** the contents of an electronic mail message when the perso. using the contents **knew or had reason to know** that the information was obtained through an illegal interception.[3]

Congress stipulated that to be illegal, the interception, disclosure or use of electronic mail must be **intentional**; thus, inadvertent interceptions are not crimes.[4] For example, if an electronic mail customer inadvertently receives a message intended for another customer, the customer who mistakenly received the message would not be subject to a prosecution. Similarly, an individual who is mistakenly connected to a telephone call is not in violation of the wiretap law. On the other hand, a hacker or corporate spy who intentionally attempts to intercept an electronic mail message would likely be prosecuted under ECPA.

Whether an interception is illegal depends on whether the act was intentional. Therefore, the definition of "intent" is vital. Congress made clear that the motive for intercepting, disclosing or using electronic mail is not to be considered in determining whether an act was intentional, only whether the act was a person's conscious objective.[5] As the Senate Judiciary Committee reported, "People who steal because they like to or to get more money or to feed the poor, like Robin Hood, all commit the same crime."[6]

2. Rules For Public Service Electronic Mail Firms

Electronic mail firms that offer service to the public, including firms that offer

Chapter 2 Interception Of Electronic Mail By Law Enforcement Officials

A. Purpose

The Electronic Communications Privacy Act (ECPA) of 1986 allows law enforcement officials who are investigating crimes to intercept electronic communications, such as electronic mail, just as law enforcement officials are permitted, under strict guidelines, to tap telephones or open first-class mail to gather evidence.

While ECPA tracks the general principles in the wiretap statute concerning government monitoring of communications, the procedures for government monitoring of electronic communications are not as stringent as those which apply to telephone wiretapping.[1] These procedural differences were included at the insistence of Justice Department officials who have long opposed the added procedural burdens contained in the wiretap act and refused to permit those burdens to be carried over into the new area of surveillance of electronic communications.[2]

The law sets out specific rules to guide electronic mail firms in determining when and how to cooperate with law enforcement authorities. ECPA also requires the government in certain circumstances to reimburse electronic mail firms for costs incurred in assisting the government in monitoring messages as part of criminal investigations. Finally, the law protects electronic mail firms from lawsuits for disclosing information to law enforcement officers engaged in a duly authorized investigation. It is especially important that electronic mail executives and employees become familiar with this section of the new law because by becoming familiar with the procedures law enforcement officials must follow and the rules for cooperating with the authorities, a firm can protect itself from lawsuits by customers alleging that the firm improperly disclosed the contents of a communication to law enforcement officials.

B. The Standards

1. When Law Enforcement Officials May Intercept Electronic Mail

Law enforcement officials generally must obtain a court order to monitor electronic communications, including electronic mail.[3] Law enforcement officials must prove four things to a judge in order to get a court order:

a. *There is probable cause that an individual has committed, is committing, or is about to commit a felony;*[4]

b. *There is probable cause that the electronic mail interception requested by authorities will produce evidence of the crime being investigated;*[5]

c. *Normal investigative procedures (i.e., normal police work other than electronic monitoring) have failed or do not appear likely to succeed;*[6] and

d. *There is probable cause that the facilities where electronic mail is to be intercepted are being used or may be used in connection with the commission of a crime or are leased to, listed in the name of, or commonly used by a person being investigated.*[7] The term "facilities" in this context does not normally mean the facilities of an electronic mail firm; rather, the language is borrowed from the wiretap act, which refers to telephones. Here "facilities" means the personal computer or terminal through which an individual gains access to an electronic mail system.

C. The Exceptions

1. Court Order Need Not Name Electronic Mail Facility If Suspect Would Be Tipped Off

In making an application for a court order, law enforcement officials do not have to identify the specific electronic mail facilities where monitoring is to be carried out if identifying the facility may tip off suspected criminals and lead them to change to another electronic mail facility. Here again, the term "facility" does not normally refer to the offices, headquarters or property of an electronic mail firm. Rather, the term refers to the computer from which illegal activity was originated, such as a persona computer. Specifically, law enforcement officials need not show that a particula personal computer is connected with a crime or used by a suspected criminal if a federal law enforcement officer with the approval of the Attorney General or other high level Justice Department officials does the following:

a. *Applies for a court order;*

b. *Identifies the person suspected of committing the crime and whose electronic mail is to be intercepted*; and

c. *Shows that the suspected criminal, if put on notice by a court order, may attempt to thwart interception by changing facilities.*[8]

These so-called "relaxed specificity" orders are meant to allow law enforcement officials to monitor the activities of criminals who move from computer to computer to avoid detection while accessing an electronic communications system. This provision follows a similar section in the wiretap act which allows authorities to monitor phone calls made by a criminal suspect on numerous public telephones to avoid surveillance. Relaxed specificity orders are considered extraordinary and require approval by the highest level officials at the U.S. Department of Justice.[9] Waiving the requirement that the government state the exact place where the interception is to occur is not meant to give law enforcement officials carte blanche to place interceptio devices everywhere and "is not considered a substitute for investigative footwork."[10] Rather, this provision was intended to prevent sophisticated suspects from discovering that interceptions have been ordered, thereby encouraging them to change the electronic mail service they use.[11]

2. *Expedited Rules For Emergency Situations*

Under normal circumstances, law enforcement officials must obtain a court order **before** they begin monitoring electronic mail transmissions. But in certain emergency situations, such as when an individual's life is at risk, high-level federal and state attorneys may authorize monitoring before a court order has been obtained.

Specifically, if specially designated federal and state law enforcement officers[12] determine that an emergency exists—an emergency which poses an immediate threat of death or injury to an individual, which threatens national security, or which is characteristic of organized crime—the strict rules concerning court orders for monitoring electronic mail transmissions can be waived.[13] In addition to showing that an emergency exists, law enforcement officials must also show that it is necessary to intercept an electronic mail transmission immediately, before a court would have time to rule on a court order.[14] Finally, law enforcement officers must conclude that a court would likely grant an order if time were available because the circumstances of the case meet the four-part test described above.[15] Within 48 hours after the interception occurs, law enforcement officials must apply for a court order.[16]

D. Procedures

1. *Cooperation Of Electronic Mail Firms With Law Enforcement Officers*

Providers of electronic communications, including electronic mail firms, are required to provide law enforcement officials all information, facilities and technical assistance necessary to accomplish an interception.[17] The firm's obligation to provide facilities and assistance is limited, however, so that the interception will be unobtrusive and will only cause a minimum of interference with the services provided by an electronic mail firm.[18] There is also a requirement that any interceptions of electronic mail messages involved in a criminal investigation will be carried out in such a way as to minimize interception of electronic mail messages not involved in the investigation.[19]

If an electronic mail firm believes that law enforcement officials are making unreasonable demands for assistance or that government monitoring is unduly interfering with the firm's ability to provide service to its customers, the firm may move to quash the court order authorizing the interception. The firm must show that it cannot provide the assistance request in a timely or reasonable fashion.[20] The Justice Department recognizes the importance of working reasonably with electronic mail and other communications firms. Then-Assistant Attorney General William F. Weld, head of the Criminal Division, wrote in 1986, "The key for all concerned is to approach this procedure with care and foresight and to be aware of the practical and legal problems which may arise."[21]

In certain cases, law enforcement officials may require the assistance of employees of electronic mail firms in setting, translating and/or decoding interceptions. Under prior law, it was necessary to deputize non-law enforcement officials who assisted and helped interpret interceptions.[22] Under the new law, there is no need to deputize assistants, but these assistants must be under contract with the government and be under the supervision of authorized law enforcement officers.[23]

Interception orders can run up to 30 days with the possibility of a 30-day extension under limited circumstances.[24] The 30-day period begins to run either when the actual interception begins or not later than 10 days after the court order is entered.[25] This leeway in starting the 30-day period is meant to provide a grace period to law enforcement officials in the event that they encounter technical difficulties in setting up the interception.[26]

2. *When To Cooperate With Law Enforcement Officers*

An electronic mail firm cannot be sued for disclosing the contents of electronic mail messages or for aiding government interception of electronic mail transmissions, if the firm relied in good faith on a **facially valid** court order, warrant or subpoena, or a request from a law enforcement officer (in those limited emergency situations where authorities must apply for a court order after the fact).[27]

Specifically, law enforcement officials must provide an electronic mail firm with a court order signed by a judge directing the firm to cooperate, or with a written statement by a specially designated law enforcement officer certifying that an emergency situation exists which did not permit authorities to obtain a court order before the fact.[28] The court order or certified statement must specify the amount of time required for the interception and must also specify the information sought and the assistance required.[29]

In order to act in "good faith" and therefore avoid a suit for disclosing electronic mail while in transmission, representatives of an electronic mail firm **must read** the court order or certification.[30] There is no need for an electronic mail firm to legally analyze the court order or certification; the order or certification must only be **facially** valid.[31] See the appendices, which include sample court orders. It is important to underscore that representatives of an electronic mail firm have a positive **duty** to read court orders, subpoenas and statements certifying that an emergency situation exists before providing assistance to law enforcement officials. Failure to do this can leave a firm defenseless against a suit by an aggrieved customer should the order prove to be defective.

An electronic mail firm must also take care to cooperate with law enforcement officials only within the confines of the court order. For example, if a court order authorizes monitoring of electronic mail messages for 30 days, a firm must not allow police officials to continue monitoring after the thirtieth day unless the police present the firm with a new court order or certification or an authorized extension. These are the same types of restrictions which apply to phone companies and to mail carriers. Similarly, if a court order specifies that law enforcement officials may monitor a specific individual's electronic mail, an electronic mail firm must not assist authorities in any way in monitoring the electronic mail of other customers not mentioned in the court order or certification, regardless of any argument that law enforcement officials make. Providing cooperation with authorities outside the scope of a court order or emergency certificate is illegal and can subject a firm to a lawsuit.

As long as electronic mail firms have acted in good faith within the bounds of a court order or certification and have not colluded with law enforcement officials, no civil suit will lie against the firm for disclosing electronic mail messages.

In addition to assisting the authorities only within the bounds of a court order, electronic mail firms must avoid the appearance of colluding with law enforcement officials. If collusion is found, a firm may not invoke the good faith defense in a suit by an aggrieved customer and could therefore expose itself to a damage award. Therefore, if an electronic mail firm has actual knowledge that law enforcement officials have not followed the proper procedures in obtaining authorization to monitor electronic mail transmissions, the firm **should not** cooperate with law enforcement officials, or it risks exposing itself to civil liability. While an electronic mail firm does not have a positive duty to investigate whether or not law enforcement officials are following correct procedures, if the firm learns that law enforcement officials have acted incorrectly, it may lose its good faith defense by continuing to cooperate with the authorities after it has learned of their illegal behavior.

ECPA includes tough provisions for lawsuits against electronic mail firms which have acted in bad faith.[32] A complaint by an aggrieved electronic mail customer must allege that an electronic mail firm (or one of its employees)

a. *Disclosed electronic mail messages to government agents without a facially valid court order or certification;* or

b. *Acted beyond the scope of the court order or certification;* or

c. *Acted in bad faith (i.e., did not read the order or colluded with law enforcement officials).*[33]

The Electronic Communications Privacy Act is very specific about the procedures a customer must follow to initiate a suit against an electronic mail firm for cooperating with law enforcement officials. If an allegedly aggrieved customer fails to follow these procedures, the new law gives electronic mail firms a chance to short-circuit lawsuits, either by moving for dismissal of the case or through summary judgment against the customer. If a complaint fails to make any of these allegations, an electronic mail firm may move to dismiss the complaint for failure to state a claim upon which relief can be granted.[34] An electronic mail firm/defendant can also move for summary judgment if, during pretrial discovery, the plaintiff's claim proves baseless.[35] If a court denies the summary judgment motion and the case goes to trial, a defendant may move for dismissal at the end of the plaintiff's case. If that motion is denied, the defendant then can present a good faith defense to the jury.[36]

3. *Who Pays For The Costs Incurred By An Electronic Mail Firm In Cooperating With Government Officials?*

Electronic mail firms are to be compensated for reasonable expenses incurred in providing facilities and technical assistance to law enforcement officials authorized to intercept transmissions.[37] Congress intended the term "reasonable expenses" to mean "an appropriate amount in light of the work required for a particular activity."[38] In ordinary cases, a flat or general rate may be appropriate, but in unusual cases the law calls for flexibility to permit reimbursement at higher levels.[39]

Therefore, electronic mail firms should take care to keep track of the number of hours that their employees must devote to assisting law enforcement officials. And to the extent that government officials require use of your systems, they should be billed at the general rate which other users must pay for on-line time.

In the event that a dispute with government law enforcement officials arises concerning the amount of compensation owed to an electronic communications firm for its cooperation, Title I of ECPA does not specifically provide a means of resolving the dispute. Certain provisions of Title II of the new law (which governs police access to electronic communications in storage), however, do provide some instruction for resolving financial differences. A reasonable argument can be made that this dispute-resolution mechanism should also be used to resolve disputes concerning the costs of assisting government efforts to intercept electronic mail in transmission.

The amount of reimbursement due to an electronic mail firm must generally be agreeable to both law enforcement officials and the firm.[40] If the firm and government officials cannot reach an agreement on the amount of compensation due, an electronic mail firm may ask a court to set a "reasonable" fee.[41] Normally, the court which issued the order directing an electronic mail firm to cooperate with law enforcement officials will resolve this sort of dispute. But in those limited cases where no court order has been issued (e.g., where an emergency situation exists and police obtain an emergency certification), the court hearing the criminal prosecution may set the fee.[42] Of course, a firm should consider the costs associated with litigation concerning the amount of compensation due before asking a court to settle the firm's differences with law enforcement authorities.

E. The Penalties For Disclosing The Existence Of An Investigation

1. It Is A Felony For An Electronic Mail Firm To Tell A Customer The Government Is Intercepting His Or Her Electronic Mail Messages

Electronic mail firms and their employees must not tell customers or any person that law enforcement officials have applied for a court order to intercept electronic mail. An electronic mail firm, employee or any individual who gives notice or attempts to give notice that the government is intercepting electronic mail is guilty of a federal felony punishable by up to five years in prison and a fine of up to $250,000 for individuals and $500,000 for organizations, or both.[43]

Specifically, there are three elements of this crime. First, an individual or entity must have knowledge that a law enforcement officer has applied for an order to intercept electronic mail or that such an order has been made by a court.[44] Second, an individual or firm must give notice of a possible interception to any person who is the target of the interception.[45] Finally, an individual or firm must give notice or attempt to give notice of the interception with the intent to obstruct, impede or prevent the interception.[46]

1. For example, under ECPA **any** attorney for the federal government (i.e., assistant U.S. attorneys all the way up to the Attorney General) may apply for a federal court order to monitor electronic communications. 18 U.S.C.A. sec. 2516(3). Under the wiretap statute, however, only high level Justice Department officials may apply for a court order to tap a telephone. S. Rep. No. 541 99th Cong., 2nd Sess., 28 (1986). Further, a court order authorizing the interception of electronic communications can be issued if a judge finds that the proposed interception would produce evidence of **any** federal felony. Telephone wiretapping can only be authorized to investigate a specific list of the most serious federal felonies. Id.

2. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All States Attorneys and Strike Force Chiefs, December 15, 1986, 8.

3. 18 U.S.C.A. sec. 2518 (West Supp. 1988).

4. 18 U.S.C.A. sec. 2518(3)(a) (1970).

5. 18 U.S.C.A. sec. 2518(3)(b).

6. 18 U.S.C.A. sec. 2518(3)(c).

7. 18 U.S.C.A. sec. 2518(3)(d) (West Supp. 1988).

8. 18 U.S.C.A. sec. 2518(11)(b) (West Supp. 1988).

9. For example, the approval of an Assistant Attorney General is required and approval by a Deputy Assistant Attorney General is unacceptable. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All States Attorneys and Strike Force Chiefs, December 15, 1986, 11, 12. On the other hand, routine applications for court orders authorizing the interception of electronic communications can be made by any attorney for the government. 18 U.S.C.A. sec. 2516(3).

10. William Weld at 12.

11. Id.

12. To be specially designated, law enforcement officials must have the approval of the U.S. Attorney General, the Deputy Attorney General, the Associate Attorney General, or an Assistant Attorney General. William F. Weld, Memorandum to All U.S. Attorneys and Strike Force Chiefs, December 15, 1986, 11, 12.

13. 18 U.S.C.A. sec. 2518)(7)(a) (West Supp. 1988).

14. 18 U.S.C.A. sec. 2518(7)(a) (West Supp. 1988).

15. 18 U.S.C.A. sec. 2518(7)(b) (West Supp. 1988).

16. 18 U.S.C.A. sec. 2518(7)(b) (West Supp. 1988).

17. 18 U.S.C.A. sec. 2518(4) (West Supp. 1988).

18. 18 U.S.C.A. sec. 2518(4) (West Supp. 1988).

19. 18 U.S.C.A. sec. 2518(5) (West Supp. 1988).

20. 18 U.S.C.A. sec. 2518(12) (West Supp. 1988).

21. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All U.S. Attorneys and Strike Force Chiefs, December 15, 1986, 12.

22. Id. at 10.

23. 18 U.S.C.A. sec. 2518(5) (West Supp. 1988).

24. 18 U.S.C.A. sec. 2518(5) (West Supp. 1988).

25. 18 U.S.C.A. sec. 2518(5) (West Supp. 1988).

26. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All States Attorneys and Strike Force Chiefs, December 15, 1986.

27. 18 U.S.C.A. sec. 2520(d) (West Supp. 1988). H.R. Rep. 99-647 at 50 explains that the court order need only appear to be facially valid.

28. 18 U.S.C.A. sec. 2511(2)(a)(ii) (West Supp. 1988).

29. 18 U.S.C.A. sec. 2511(2)(a)(ii)(B) (West Supp. 1988).

30. S. Rep. No. 541, 99th Cong., 2nd Sess., 26 (1986).

31. S. Rep. No. 541, 99th Cong., 2nd Sess., 26 (1986).

32. 18 U.S.C.A. sec. 2520(a) (West Supp. 1988).

33. S. Rep. No. 541, 99th Cong., 2nd Sess., 26 (1986).

34. S. Rep. No. 541, 99th Cong., 2nd Sess., 26 (1986).

35. Id.

36. S. Rep. No. 541, 99th Cong., 2nd Sess., 26, 27 (1986).

37. 18 U.S.C.A. sec. 2518(4) (West Supp. 1988).

38. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 52 (1986).

39. Id.

40. 18 U.S.C.A. sec. 2706(b) (West Supp. 1988).

41. S. Rep. No. 541, 99th Cong., 2nd Sess., 43 (1986).

42. 18 U.S.C.A sec. 2706(c) (West Supp. 1988).

43. The Electronic Communications Privacy Act, Pub. L. 99-508, sec. 109 (October 21, 1986).

44. S. Rep. No. 541, 99th Cong., 2nd Sess., 34 (1986).

45. Id.

46. Id.

Chapter 3 Protecting Electronic Mail In Storage

A. Purpose

Title II is the core of the Electronic Communications Privacy Act. Title II establishes entirely new rules specifically designed to protect the privacy and security of electronic communications systems. These important provisions are divided into two main parts: 1) those which protect electronic mail systems from hackers and other individuals who try to break through computer security systems; and 2) those provisions that safeguard stored electronic mail messages from unauthorized government access.

This chapter describes the provisions of ECPA intended to protect electronic mail systems from private individuals, whether hackers or high-tech thieves, who attempt to gain access to information stored in electronic mail systems.

In general, ECPA protects electronic communications systems by making it a federal felony to access an electronic communications system without authorization and then steal information or cause damage to the system.[1] In addition, ECPA makes it a crime for an individual who is authorized to gain access to certain parts of an electronic mail system to exceed his or her authorization, enter restricted parts of the system, and obtain information or generally cause damage to the system.

It is important to note that the protections afforded to stored communications not only apply to electronic mail messages in an individual user's mailbox, but also to messages stored temporarily prior to forwarding and messages maintained in a backup system.

Title II of ECPA protects electronic mail and remote computing systems by creating a strong deterrent against intruders. Violators can be punished by up to one year in federal prison and fines of up to $250,000. By helping to safeguard electronic communications systems, the new law affords electronic mail providers the opportunity to further develop their businesses and to assure customers that their communications will remain secure.

B. The Standard

1. Intentional Access Of Electronic Mail Systems Without Authorization

It is illegal to intentionally access an electronic mail system or electronic communication service without authorization.[2] A number of tests must be met to determine whether a breach of the law has occurred.

The first test is whether the access was **authorized**. There is no specific definition of authorized access provided in the law. In May of 1989, FBI Director William Sessions testified before the Senate Subcommittee on Technology and the Law that the lack of a definition for "authorized access" may impair the efforts of prosecutors to pursue cases under ECPA and the Computer Fraud and Abuse Act (CFAA) which similarly lacks a definition of authorized access.[3] Congress is considering adding a statutory definition of authorized access for both the CFAA and ECPA. In the meantime, the case of Robert T. Morris may provide guidance as to how the courts will interpret the unauthorized access provisions of ECPA.[4] On January 22, 1990, Morris, a Cornell University computer science graduate student, was convicted in perhaps the most publicized case of computer crime. Morris planted a computer worm in the Internet computer network and caused up to $10 million in damage to computers across the country.[5] Valuable information and files were lost and entire systems were forced to shut down for hours.

While the Morris case was prosecuted under the Computer Fraud and Abuse Act of 1984,[6] this case will likely have significant implications for Title II of ECPA. The CFAA includes protections similar to those in ECPA, and the Morris case, once appeals are concluded, may offer guidance as to how the courts will handle litigation under both laws. The CFAA is largely aimed at protecting federal government, defense, medical and financial institution computers, while ECPA is designed to protect electronic communications systems from intruders.

A strong argument can be made that industry standards for authorized use of electronic communications systems should be used to interpret the unauthorized access test in ECPA. Most electronic mail and other electronic communication service providers have protections built into their systems such as basic passwords and fees for usage. Thus, most electronic mail services have a system for identifying customers who are explicitly authorized to use the system. Those without passwords and those not paying for the services are generally not permitted to use them, and should generally be considered unauthorized users in the context of this law.

Congress did not intend, however, to prohibit authorized users from sharing their passwords with others and thereby explicitly authorizing them to access a system.[7]

While the legislative history does not define unauthorized access to an electronic mail system, it does clarify that accessing an electronic bulletin board that is intended to be open to the public is exempt from the unauthorized access provision.[8] In this case, Congress clearly sought to acknowledge the industry standard of allowing relatively free access to electronic bulletin boards.

Until Congress and the courts clarify the definition of authorized access, electronic mail firms can take certain steps to increase the likelihood that intruders will be successfully prosecuted. In general, by building security and explicit authorization points into an electronic mail system and by making the rules of authorized access plainly known (as most responsible firms already do), public service electronic mail firms and managers of internal messaging systems can help federal prosecutors prove that intruders gained access to a system without authorization.

The second test in the law is that the access must be **intentional**.[9] While this section of the law does not define intent, intent is defined in the legislative history covering other provisions of the new law. Intent is defined as knowingly committing an act.[10] Therefore, in order to prove a case under ECPA, prosecutors must demonstrate that an individual had the "conscious objective" of gaining access to an electronic mail system.[11] But it is not necessary to prove that an individual intended a harmful result —only that the individual intended to gain access. For example, a hacker who makes a conscious effort to break into an electronic mail system would be considered to have shown the requisite intent.[12] On the other hand, an individual who gains access to an electronic communications system by misdialing a telephone number would very probably not meet the test of intentional access.

2. Intentionally Exceeding Authorization To An Electronic Mail System

It is also illegal under this statute for an individual to exceed the authorization he or she has been given to an electronic mail facility.[13] This provision is designed to address two specific types of circumstances.

First, ECPA makes it illegal for a user who is authorized for access to **his or her** own stored electronic mail messages to intentionally exceed that authorization and thereby gain access to the electronic mail of other users or information maintained by an electronic mail firm.[14] The law is equally applicable to other types of electronic communications systems. For example, it is illegal for an individual who is authorized to access an account on a financial services communications system to exceed that authorization and obtain information from another individual's account.

Second, this provision is applicable to those electronic communication systems that have both public and private components. On many systems, individuals have private electronic mail message boxes, but are also given broad access to electronic bulletin boards or other public systems in which all users on a system may exchange messages. The portions with no access barriers or where any user may gain access simply by a self-assigned password are considered public, and therefore accessing these sections would not constitute a violation.[15] However, accessing any portion of the system not intended for public disclosure would constitute a violation, provided that the access results in disclosure.[16]

Under this provision of ECPA, for example, it is illegal for an individual to exceed his or her authorization to use an electronic bulletin board in order to gain access to other private electronic mail files or to gain access to information stored by the electronic mail provider.

3. *Unauthorized Access Must Result In Disclosure To Be Considered A Crime*

The third criterion for proving a crime under ECPA is that unlawful access must result in the intruder **obtaining, altering or preventing access** to a stored electronic communication.[17] This criterion applies both when an individual accesses an electronic mail system without authorization and when an individual exceeds his or her authorization.

The first two forms of illegal activity—obtaining or altering information—are relatively straightforward. If an intruder illegally gains access to an electronic mail system and obtains information or manipulates information in the system, the intruder is guilty of a crime.

The third form of illegal activity—preventing access to a stored electronic communication—may be more difficult to prove. As in the case of the Cornell Worm, intruders who illegally gain access to a computer system may cause the system to slow down or even to shut down completely. As a result, electronic mail users may be prevented from accessing their messages. This is a relatively straightforward example. It may be more difficult to prove that an intruder prevented access to a stored communication, where the intruder merely slows down the workings of a computer system either by manipulating files or inserting commands that slow the system down. Finally, in some instances an intruder may intentionally attempt to prevent an electronic mail user from gaining access to his or her specific electronic mail file. This clearly is the type of activity that ECPA seeks to outlaw.

C. The Exceptions

The statute provides a number of common sense exceptions to the unlawful access provisions. These provisions make it possible for electronic mail and electronic communication services to operate successfully, while ensuring the integrity and privacy of their systems.

1. *Electronic Mail Systems Generally Available To The Public*

The Electronic Communications Privacy Act does not prevent access to public electronic communication facilities or services. It does not hinder development or use of such services as electronic bulletin boards and similar services intended for broad public use.[18] These services include those in which interested persons may communicate openly to exchange opinions or computer programs in the public domain.[19] In these services, the sender is generally deemed to have extended authorization to the public for access to the communication.[20]

Electronic bulletin boards and other similar services are distinguished by broad public knowledge of entry to the system. This includes wide knowledge of the telephone number and other means of access. It also means that the user does not, in the course of gaining entry to the communication, encounter any warnings, encryptions, password requests, or other indicators of intended privacy.[21] Authorization to such systems is considered implicitly provided, and therefore it is not a violation of the law to use these systems.[22] In addition, privacy is generally not expected by either the provider or the user for the communications sent over the system, at least with respect to messages sent on the open part of the system. As mentioned previously, some systems have private elements and a public electronic bulletin board element. While messages sent via the electronic bulletin board are not subject to the rules against disclosure, messages sent on the private element of the electronic communications system are subject to the restrictions.

2. *Access Authorized By The Service Provider*

A common sense exception is provided, under which firms providing electronic mail or other electronic communication services are entitled to provide authorization to users of their services.[23] This provision makes it possible for electronic mail and electronic communications services to provide customers or subscribers with a private means of communication. The provider is allowed to construct as many security barriers as it deems necessary to adequately protect the type of communication service being offered.

3. *Authorization Provided By The Customer*

Customers of electronic mail systems may authorize others to access their own stored communications.[24] For example, a business executive who uses an electronic mail system may authorize an assistant to access the stored communications in his or her electronic mailbox. The assistant would not be in violation of the law if permission is given.

4. *Authorization Pursuant To A Lawful Court Order Or Warrant*

Finally, electronic mail providers may disclose stored communications to law enforcement authorities who present valid court orders and warrants.[25] See Chapter 5, which deals exclusively with the extensive procedures created by ECPA concerning requests by law enforcement officials for stored electronic communications.

D. The Penalties

The statute distinguishes between two classes of violations: 1) those for commercial advantage, malicious destruction, malicious damage or private commercial gain; and 2) all other forms of violation. Violations of the first class carry a much stiffer penalty. This distinction was intended to treat computer hackers who have relatively less malicious intentions differently from individuals who purposefully gain access to an electronic mail system to steal or cause destruction.

1. Violation For Private Gain, Malicious Destruction, Etc.

A person who intentionally accesses electronic mail or other electronic communications systems for private or commercial gain, malicious destruction, or damage of a communication is subject for a first offense to a maximum fine of $250,000, or a jail sentence of not more than one year, or both.[26] Any subsequent offense under this title is subject to the same fine provision, and up to a two-year jail term.[27]

The stiff penalties under this section of the law make it very clear that commercial espionage is just as illegal if conducted through computer systems as if it is done through telephone wiretaps. In addition, this section would apply to disgruntled employees and any other persons who use illegally obtained electronic communications for their own gain, or to damage in some way the addressee, sender or system provider.

2. All Other Violations

Any violation of this statute that is neither for private or commercial gain nor for malicious destruction or damage carries lesser penalties. This lesser penalty generally applies to computer hackers who gained access illegally, but did so for the purpose of gaining access itself, rather than obtain or manipulate the specific documents or stored communications which were accessed. The maximum penalty is a fine of $5,000, up to six months in prison, or both.[28] The statute does not specify stiffer penalties for multiple offenses.

Endnotes Chapter 3

1. 18 U.S.C.A. sec. 2701(a) (West Supp. 1988).

2. 18 U.S.C.A. sec. 2701(a)(1) (West Supp. 1988).

3. William S. Sessions, Director of the Federal Bureau of Investigation, Testimony Before the Subcommittee on Technology and the Law, Senate Committee on the Judiciary, May 15, 1989.

4. Statement of Computer and Business Equipment Manufacturers Association to the Subcommittee on Technology and the Law, May 19, 1989, 5.

5. General Accounting Office, Computer Security: Virus Highlights Need for Improved Internet Management, GAO.IMTEC 89-57, 17.

6. 18 U.S.C.A. sec. 1029 (West Supp. 1988).

7. S. Rep. No. 541, 99th Cong., 2nd Sess., 36 (1986).

8. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 62, 63 (1986).

9. 18 U.S.C.A. sec. 2701(a)(2) (West Supp. 1988).

10. S. Rep. No. 541, 99th Cong., 2nd Sess., 23, 24 (1986).

11. Id.

12. S. Rep. No. 541, 99th Cong., 2nd Sess., 36 (1986).

13. 18 U.S.C.A. sec. 2701(a)(2) (West Supp. 1988).

14. S. Rep. No. 541, 99th Cong., 2nd Sess., 36 (1986).

15. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 63 (1986).

16. S. Rep. No. 541, 99th Cong., 2nd Sess., 36 (1986).

17. 18 U.S.C.A. sec. 2701(a) (West Supp. 1988).

18. S. Rep. No. 541, 99th Cong., 2nd Sess., 36 (1986).

19. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 62 (1986).

20. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to all U.S. Attorneys and Strike Force Chiefs, December 15, 1986, 15.

21. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 62 (1986).

22. S. Rep. No. 541, 99th Cong., 2nd Sess., 36 (1986).

23. 18 U.S.C.A. sec. 2701(c)(1) (West Supp. 1988).

24. 18 U.S.C.A. sec. 2701(c)(2) (West Supp. 1988).

25. 18 U.S.C.A. sec. 2701(c)(3) (West Supp. 1988).

26. 18 U.S.C.A. sec. 2701(b)(1)(A) (West Supp. 1988).

27. S. Rep. No. 541, 99th Cong., 2nd Sess., 36 (1986).

28. 18 U.S.C.A. sec. 2701(b)(2) (West Supp. 1988).

Chapter 4 The Rule Against Disclosure Of Contents In Storage

A. Purpose

While Title II of the Electronic Communications Privacy Act affords electronic mail providers substantial **benefits** by protecting electronic mail systems from outside intruders, this portion of ECPA also imposes significant **legal responsibilities** specifically on entities that provide electronic mail and remote computer services to the public. This provision of ECPA creates the potential for legal exposure, and therefore it is important that electronic mail executives and employees become familiar with the new rules. This chapter explains the responsibilities of electronic mail firms under Title II of ECPA.

Title II is designed specifically to protect users of electronic communications systems by generally preventing firms providing electronic mail service to the public from disclosing the contents of their customers' messages to third parties, except under circumstances defined by the law. By preventing the disclosure of messages by electronic mail providers, ECPA affords privacy protection to electronic communications similar to that afforded to telephone conversations. These restrictions apply to electronic mail messages in storage, while other parts of the law protect the privacy of messages while in transmission. (See Chapter 1.)

Specifically, Title II of ECPA makes it illegal for a person or entity providing an electronic communications service to the public to knowingly divulge the contents of electronic communications in storage.[1] This chapter will explain this standard, including what is meant by to "knowingly divulge" an electronic mail message.

Title II does not impose a complete ban on the disclosure of electronic mail messages in storage. To ensure that electronic communications providers may continue to efficiently serve their customers, Congress included a number of commonsense exceptions to the rule against disclosing contents. The exceptions are discussed below.

Title II puts teeth into the new rules by creating a cause of action under which electronic mail users may sue electronic mail firms for disclosing the contents of electronic mail messages in violation of the law. In an effort to protect electronic mail firms from frivolous litigation, however, ECPA sets out a number of legal defenses under which an electronic mail firm may defend its decision to disclose the contents of an electronic mail message, as permitted by law.

While the rule against divulging contents would appear to create added burdens on electronic mail providers, the rule also directly benefits the electronic mail industry. By guaranteeing the privacy of electronic communications—by ensuring that electronic mail firms will not disclose commercial information to competitors, for example—ECPA provides an incentive for businesses and individuals to use electronic mail.

B. The Standard— To "Knowingly Divulge"

Under the Electronic Communications Privacy Act, it is unlawful for providers of electronic communications services or remote computing services to "knowingly divulge to any person or entity the contents of a communication while in electronic storage."[2] Of course, the law provides certain exceptions, which are discussed below, but first it is important to understand the tests set out for meeting the standard.

The first test is whether an electronic mail firm "knowingly divulged" a communication. To knowingly divulge is to act with intention. An electronic mail firm only exposes itself to a lawsuit by disclosing the contents of a message when the firm is aware that it is disclosing the message to a person other than the intended recipient or another party excepted under the law, such as an intermediary involved in forwarding messages.

In legal parlance, an electronic mail firm that exhibits "willful blindness" in disclosing a message to an inappropriate party is guilty of a violation, while negligently disclosing a message does not fall within the definition.[3]

In simple terms, in order to guard against a lawsuit, an electronic mail firm shoul take steps to ensure that its employees do not intentionally disclose the contents of electronic mail messages to anyone other the addressee or the other parties excepted under the law, such as intermediaries.

The second test is whether an electronic mail firm has disclosed the **contents** of an electronic communication as defined in ECPA. The contents of an electronic communication are considered to be the substance of a message or the effect or meaning of a communication.[4] This test is intended to allow electronic mail firms to disclose some information to third parties about electronic mail messages, while protecting the confidentiality of the actual substance of the message or series of messages. For instance, an electronic mail firm may disclose transactional information or broad, generalized demographic information about its users as a marketing tool, but is prohibited under the act from disclosing information about a specific client's messages unless the client gives its approval.

1. ECPA Rule Against Disclosure Does Not Interfere With Other Disclosure Laws

It is important to note that the new rule against disclosing the contents of electronic communications does not relieve providers of either wire or electronic communications from their obligations under other laws, including the Fair Credit Reporting Act.[5] company's duties under the Fair Credit Reporting Act, which limits consumer reporting agencies in disclosing financial information under certain circumstances, are not affected in any way by this law.[6]

Companies that provide both electronic communication services and other services to the public would be governed by separate disclosure laws. If a company provided both electronic mail and credit rating services, the electronic mail disclosure would be regulated by the Electronic Communications Privacy Act, while the credit rating services would be governed by the Fair Credit Reporting Act.[7] If another law covering another area of a corporation's business would not allow disclosure of the information, non-disclosure would be the appropriate outcome.[8]

2. Special Standard For Remote Computing Services

Remote computing services are prohibited from "knowingly divulging" the contents of any communication **carried or maintained** by that service on behalf of a subscriber or customer.[9] Therefore a remote computing firm may disclose the contents of communications that it creates itself, but must not disclose the contents of communications it receives from customers. Further, remote computing firms are only limited in their ability to disclose information that is transmitted via electronic communication from a customer. For example, ECPA would prevent the disclosure of raw data sent electronically to a remote computing firm by a client for processing and computing. But if a computer tape is sent through the mail for processing, the disclosure of the contents of the tape by the remote computing firm would not be a violation of ECPA, but may be subject to restrictions under other laws.[10]

C. The Exceptions

The Electronic Communications Privacy Act sets out numerous exceptions to the rule against disclosing the contents of communications, under which electronic mail firms may disclose their customers' messages without exposing themselves to litigation.

1. The Obvious Exception

It is, of course, permissible under ECPA to disclose the contents of a stored electronic communication to the addressee or intended recipient of the communication, or an agent of that addressee or recipient.[11] A person does not need to be individually identified in order to be an intended recipient of a communication. For example, the communication could be addressed to the members of a group. Any member of the group, whether individually named or not, would be considered an intended recipient of the communication and an electronic mail firm would not be liable under the Act for making such a disclosure.[12]

In the case of operators of electronic bulletin boards, a firm may disclose the contents of a message to anyone reasonably considered a part of the group addressed in the communication.[13]

When a customer or subscriber places a communication on the service, but does **not specify the name of the addressee,** an electronic mail firm may disclose the contents of the communication without exposing itself to litigation. This would only occur in the bulletin board context. On traditional electronic mail systems, unaddressed messages would not be forwarded to anyone unless an address is given. In the bulletin board context, the failure to identify the addressee of a message makes an electronic communications firm the *de facto* addressee. And since an addressee may give consent to disclose the contents of a communication, under the law an electronic mail firm may legally disclose the message.[14]

2. Disclosure With Consent

An electronic mail firm may disclose the contents of a message in storage if the sender, addressee or intended recipient gives consent.[15] With the consent of subscribers, remote computing services may disclose the contents of communications.[16] Consent may be obtained either through a formal written document or through an electronically transmitted grant of consent.[17] Electronic mail providers should review the language of their service contracts and consider amending them to ensure that the terms for disclosing stored messages are consistent with the provisions of the new law

Consent need not be explicit, however, and may be inferred in some instances.[18] The legislative history of ECPA identifies a number of circumstances in which consent may be inferred. It is important to note, however, that the circumstances under which consent may be inferred depend strongly on the facts of the case.

An electronic communications firm may infer that consent to disclose the contents of a communication has been given when

a. *A history of transactions provides a reasonable basis for inferring that a certain class of communications may be disclosed.*[19] For example, if the intended recipient of the communication is an executive who routinely authorizes his or her secretary to "pick up" electronic mail messages, it could be inferred that disclosure to the secretary is consented to, and therefore the disclosure would be lawful.

b. *A customer or subscriber may reasonably be expected to understand that disclosure may take place, and acknowledges such circumstances through continued use of the service, such as an electronic bulletin board.*[20]

c. *A customer uses an open access electronic bulletin board, it is implied that the customer has reasonable knowledge that communication will be freely available to the public, and therefore consent to disclose the communication is automatically implied.*[21]

d. *An electronic mail firm and its customer enter into a contract that contains provisions making it clear that the firm may disclose the contents of messages.*[22]

3. Disclosure To Those Involved In Forwarding Communications

With the era of interconnection upon us, electronic mail and other electronic communications must frequently be sent from one service provider to another in order to reach the intended recipient. In those instances, ECPA permits an electronic mail firm to disclose the contents of stored communications to persons employed or authorized by the service provider to receive communications for the sole purpose of forwarding to the addressee.[23]

4. Disclosure If Necessary To Provide Electronic Mail Service

The contents of a communication may be disclosed if it is necessary to the provision of electronic mail or other electronic communication service, or to protect the rights or property of the service provider.[24] Under this exception, an electronic mail firm may disclose the contents of a communication from one employee computer operator to another, if this is necessary to provide electronic communications services. In addition, an electronic mail firm may **randomly** monitor communications as part of its quality control operations or to mechanically maintain its system, but is not entitled to purposefully monitor the communications of a particular customer.[25] It is therefore illegal for an electronic mail firm or its employees to regularly read the contents of communications in storage. Electronic mail providers are responsible for ensuring that their employees understand the differences between random monitoring necessary to providing service and regularly monitoring and reading customers' messages.

5. Disclosure To Law Enforcement Officials

Providers may disclose the contents of a communication to a law enforcement agency without a warrant only if two conditions are met:

- The contents were **inadvertently** obtained by the provider; **and**

- The contents appear to pertain to the commission of a crime.

Government access to stored communications is dealt with extensively in the next chapter. It is important to note here, however, that Congress intended this exception to be read very narrowly. In order to prevent exposing itself to litigation, an electronic mail firm may not systematically search all the communications stored on its system to identify incriminating material. Only information that an electronic mail firm finds inadvertently may be turned over to law enforcement authorities voluntarily. In essence, this provision of the law suggests that an electronic mail firm need not ignore incriminating information that it happens upon, and may contact the authorities. For a further discussion concerning the procedures for turning information over to law enforcement authorities, see the next chapter.

D. The Penalties

ECPA does not establish any criminal penalties against an electronic mail firm for disclosing the contents of **stored** electronic communications, as opposed to electronic mail in transmission. (See Chapter 1 for the penalties that apply to the interception of messages in transmission.) But the law does create a cause of action under which electronic mail users may sue electronic mail firms for disclosing messages in violation of ECPA.[28]

1. Cause Of Action

ECPA provides for civil suits against anyone violating the disclosure provisions of the Act, including electronic mail and other electronic communication service providers and the government.[29] Suits may be brought by service providers, subscribers and customers.

This provision can work both ways for electronic mail providers. On one hand, it affords a service provider an opportunity to protect its system from unlawful disclosures, and to recover damages should an illegal disclosure occur. On the other hand, electronic mail providers can be sued for illegal disclosure of stored communications unless they are careful to follow the procedures explained above and in the next chapter.

2. Statute Of Limitations

There is a two-year deadline for filing lawsuits under this provision. The action must be commenced no later than two years after the date upon which the aggrieved party first discovered or had reasonable opportunity to discover the violation.[30] In other words, if a firm discloses the content of a customer's electronic mail messages, the customer has up to two years from the time he or she discovered the disclosure to file suit against the provider.

3. Types Of Relief Available

ECPA provides for three types of relief which an aggrieved party may seek for violations of the disclosure provisions of the statute:

• Temporary restraining orders and injunctions to prevent the illegal disclosures from continuing;[31]

• Damages as specified below; and[32]

• Reasonable attorney's fees and other litigation costs.[33]

4. *Damages Available*

An electronic mail customer may seek damages to compensate for losses resulting from an illegal disclosure by an electronic mail firm. The court may award damages up to the sum of actual damages suffered by the plaintiff and any profits made by the violator as a result of the illegal disclosure.[34]

5. *Minimum Statutory Damages*

Any plaintiff bringing charges under ECPA who is found by a court to have a valid claim is entitled to recover at least $1,000 in damages,[35] regardless of the amount of actual damages incurred.

E. Defenses Against Lawsuits

ECPA provides electronic mail and other electronic communications firms with a series of defenses against lawsuits by aggrieved customers alleging illegal disclosure of stored communications.

1. *Defense For Cooperating With Law Enforcement Authorities*

It is a complete defense that an electronic mail firm disclosed the contents of communications to law enforcement officials in good faith reliance on a warrant. The good faith defense is explained in greater detail in the next chapter.

In general, an electronic mail firm may employ the good faith defense when law enforcement officials present a warrant directing the firm to turn over the contents of a message.[36] An electronic mail firm is not required to do an in-depth legal analysis of the warrant, but it must appear to be facially valid.

In this manner, a firm can protect itself against litigation by invoking the defense that it relied in good faith on a facially valid request for information by a law enforcement officer. It is important to note, however, that the good faith defense may not be invoked when an electronic mail firm is shown to have acted in collusion with the authorities. For example, if a warrant appears to be defective on its face or if the firm is aware that law enforcement officials are acting improperly, a firm should not disclose electronic mail messages to the authorities.

2. *Defense For Relying On ECPA Exceptions*

It is also a complete defense that an electronic mail firm relied in good faith on the exceptions set out in ECPA that allow the disclosure of communications to certain parties, including addressees and forwarders of communications. It is further a defense that a firm relied on the exception permitting the disclosure of incriminating information that was inadvertently obtained by a communications provider.[37]

1. 18 U.S.C.A. sec. 2702(a)(1) (West Supp. 1988).
2. 18 U.S.C.A. sec. 2702(a)(1) (West Supp. 1988).
3. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 64 (West Supp. 1988).
4. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 64 (1986).
5. S. Rep. No. 541, 99th Cong., 2nd Sess., 37 (1986).
6. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All U.S. Attorneys and Strike Force Chiefs, December 15, 1986, 16.
7. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 65 (1986).
8. S. Rep. No. 541, 99th Cong., 2nd Sess., 37 (1986).
9. 18 U.S.C.A. sec. 2702(2) (West Supp. 1988).
10. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 66 (1986).
11. 18 U.S.C.A. sec. 2702(b)(1) (West Supp. 1988).
12. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 67 (1986).
13. Id.
14. Id. at 66, 67.
15. 18 U.S.C.A. sec. 2702(b)(3) (West Supp. 1988).
16. Id.
17. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 66 (1986).
18. Id.
19. Id.
20. Id.
21. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 66 (1986).

22. Id.

23. 18 U.S.C.A. sec. 2702(b)(4) (West Supp. 1988).

24. 18 U.S.C.A. sec. 2702(b)(5) (West Supp. 1988).

25. 18 U.S.C.A. sec 2511(2)(a)(i) (West Supp. 1988).

26. 18 U.S.C.A. sec. 2702(b)(6)(A), (B) (West Supp. 1988).

27. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 67 (1986).

28. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All U.S. Attorneys and Strike Force Chiefs, December 15, 1986, 18.

29. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 74 (1986).

30. 18 U.S.C.A. sec. 2707(e) (West Supp. 1988).

31. 18 U.S.C.A. sec. 2707(b)(1) (West Supp. 1988).

32. 18 U.S.C.A. sec. 2707(b)(2) (West Supp. 1988).

33. 18 U.S.C.A. sec. 2707(b)(3) (West Supp. 1988).

34. 18 U.S.C.A. sec. 2707(c) (West Supp. 1988).

35. 18 U.S.C.A. sec. 2707(c) (West Supp. 1988).

36. 18 U.S.C.A. sec. 2707(d)(1) (West Supp. 1988).

37. 18 U.S.C.A. sec. 2707(d)(3); 18 U.S.C.A. sec. 2511(c) (West Supp. 1988).

Chapter 5

When The Government Comes Calling

A. Purpose

This section of the Electronic Communications Privacy Act spells out the circumstances under which persons or entities providing electronic mail and other electronic communications services to the public as well as those providing remote computing services may disclose the contents of stored electronic communications to the government. It also discusses to whom and how transactional records may be disclosed.

ECPA makes several distinctions in its treatment of stored communications. The first distinction is between types of services—those which are primarily electronic communications in themselves, such as electronic mail, and those services provided by remote computing services. Within the electronic mail category, a distinction is made based on length of time in storage.

B. The Standards For Government Access To The Contents Of Stored Communications

Electronic communications stored less than 180 days are treated differently from those stored more than 180 days under the Electronic Communications Privacy Act. If a communication is in storage for less than 180 days storage by the communication's provider, it is generally considered to be related to the transmission of the communication.[1] Such stored communications are treated in a manner similar to first-class mail and are given a relatively high degree of privacy protection.[2]

Electronic communications stored more than 180 days are considered a form of backup document necessary to the integrity of the system,[3] or for the convenience and benefit of the system user.[4] Such records are treated more like business records maintained in storage by a third party. Congress thus deemed these communications less deserving of privacy protection.[5]

Electronic mail providers were specifically considered in drawing this distinction, as electronic mail communications are the most like first-class mail.[6] Electronic mail communications stored less than 180 days are subject to stiffer disclosure standards than other types of communications.

1. Electronic Communications — Electronic Mail

a. *Contents Stored Less Than 180 Days*

A government agency may obtain access to the contents of electronic communications stored less than 180 days only pursuant to a properly issued federal or state warrant.[7] An electronic mail provider has a responsibility to provide access for government officials presenting state or federal warrants, but disclosure without being presented with a warrant could subject the provider to civil liability. **Electronic mail**

providers, however, are under no obligation to routinely store documents for any period of time. Service providers need only read the warrant and determine that it **appears** to be valid in order to be protected from legal action by complying with the government request.

This provision is crucial to electronic mail providers since most documents stored on such systems are only stored for six months or less.

b. *Contents Stored More Than 180 Days*

Most electronic mail providers do not maintain stored electronic communications for longer than 180 days. The law **does not** require that communications be stored for longer than 180 days. However, if electronic mail providers or providers of other electronic communication services do store their messages for longer than 180 days, the government can more easily gain access to these files and need not obtain a federal warrant. Therefore, in developing electronic mail systems, firms should consider whether they wish to regularly store messages for longer than 180 days and thereby potentially make those messages more readily accessible to government officials.

Law enforcement officials seeking access to electronic communications stored longer than six months must choose whether they want to notify the subscriber or customer of the request. That decision determines what type of order the agency or official must obtain in order to gain access to the records.

The government has two options if it does **not** wish to notify the subscriber or customer that the government is interested in the contents of the communications: 1) obtain a search warrant; or 2) delay notice under procedures set out in the law.[8]

If the government agency does give prior notice to the customer or subscriber, the agency must

• Obtain an administrative subpoena or grand jury subpoena properly authorized by state or federal authorities;[9] or

• Obtain a court order, provided the requesting agency can show there is reason to believe the contents of the electronic communication sought pertain to a legitimate law enforcement inquiry.[10]

If a government agency or official requests access to records **stored longer than six months** and does not present a search warrant for such access, it is the **provider's responsibility** to ascertain whether notice has been provided to the customer or not. Therefore, if a law enforcement official asks an electronic mail firm to turn over a message stored for more than 180 days without producing a warrant, an electronic mail firm should withhold the stored message until the law enforcement officials verify, preferably in writing, that notice has been given or that notice has been delayed. If notice has not been given, and the procedures for delaying notice discussed below are not invoked, the provider is not obligated to comply with the government request.

Court orders requested by state government officials from state courts may only be issued in compliance with state laws.[11] If, for example, a state law or constitution requires a standard of proof other than relevance to a law enforcement inquiry in order for a state judge to issue a court order, state law enforcement officials must meet the state standard.[12] The opposite is true for federal officials, where the Supremacy Clause of the U.S. Constitution specifies that federal law supersedes state law when federal officials are involved.[13] Although it is important to be aware of these factors, it is not the service provider's responsibility to know whether the court order has been issued in accordance with the appropriate state or federal law. The order presented need only appear to be valid and correct for providers to comply and be protected from legal action.

2. Access To Communications In Remote Computing Services

A government agency may only require access to the contents of information in remote computing services if the electronic communication maintained on the service

- Was received by means of electronic transmission from the subscriber or customer, and/or was created from an electronic transmission by the remote computing facility;[14] and

- Was provided by the customer only for storage or processing purposes to the computing service, which does not have access to the contents of the communications for any other purpose.[15]

A plain reading of the law indicates that stored communications in remote computing services are not subject to the 180-day rule, and therefore government officials may obtain access to the contents of communications stored at remote computing services **at any time** with either a warrant, administrative or grand jury subpoena, or court order,[16] as described above for electronic mail stored longer than 180 days.

The Justice Department, however, points out that the legislative histories are somewhat contradictory on the 180-day rule and remote computing facilities.[17] The Department notes that the House Committee Report distinguished between the treatment of electronic communications (electronic mail) and communications to remote computing services. That report seems to support, in the Justice Department's opinion the view that since electronic communications to remote computing services are no held for purposes of transmission, they are not governed by the 180-day rule.[18]

The controversy arises from the Justice Department's reading of the Senate Committee Report, which does not make the clear distinction between electronic mail and remote computing services and which does not treat these two services separately.[19] A court could, therefore, construe the Act to mean that electronic communications stored in remote computing services are subject to the 180-day rule, which requires the federal government to obtain a search warrant in order to gain access to communications stored for less than 180 days. The government need only obtain an administrative or grand jury subpoena to gain access to communications stored for more than 180 days.

Since a plain reading of the statute, however, indicates that the 180-day rule does **not** apply, and because there has been no litigation in this area to guide remote computing firms, a firm may grant law enforcement officials access to communications in a remote computing service, regardless of the length of storage, if officials present either a grand jury or administrative subpoena. A remote computing firm need not demand that a warrant be presented in order to avoid liability under the Act. ECPA provides for a defense against civil actions when a firm has relied in good faith on the statute. Clearly, the statute can be read in good faith as not requiring a warrant. (See below for further discussion of defenses.)

3. Delayed Notice

a. *Court Order*

A government agency seeking access to electronic communications stored longer than 180 days or stored in a remote computing facility may, when applying for a court order, request delaying notification to the customer by up to 90 days. The court is required to grant such delayed notification if it determines that notification will result in an adverse consequence.[20] Extensions of up to 90 days may be granted by the court if the agency submits a new application.[21] Service providers should request copies of granted requests for delayed notification, as such documents would be important in proving a good faith reliance defense in court, should such a need arise.

b. *Administrative Or Grand Jury Subpoena*

A government agency seeking to use an administrative or grand jury subpoena, either state or federal, may delay notification for up to 90 days with the written certification of a supervisory official that notification will result in adverse consequences.[22] Under this provision, government certification is sufficient to trigger delayed notification, unlike under other laws, such as the Right to Financial Privacy Act,[23] where more extensive proof is required.

The government agency using this form of delayed notification must maintain a true copy of the certification.[24] It would be in the service provider's interest to maintain a copy of such certification as well.

The following supervisory officials are authorized to provide such certification:

- Investigative agent in charge;
- Assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office; or
- Chief prosecuting attorney or first assistant prosecuting attorney or equivalent.[25]

Examples of the types of officials who could authorize delayed certification include the Special Agent in Charge or Assistant Special Agent in Charge of an FBI or DEA office.[26]

Extensions of the 90-day delay under certification may also be granted with renewed certification that notice would cause one of the conditions outlined below.[27]

c. *Adverse Results*

Adverse results that could trigger delayed notification are delineated in the Act as well. In order for delayed notification to be granted by a court or properly certified by a supervisory official of the government agency, the judge or official must be convinced that notification would result in one of the following five circumstances:

- Endangering the life or physical safety of an individual;

- Flight from prosecution;

- Destruction of or tampering with evidence;

- Intimidation of potential witnesses; or

- Otherwise seriously jeopardizing an investigation or unduly delaying a trial.[28]

If any of these conditions exist, the government agency may, through the procedures noted above, delay notifying the customer or subscriber that it is interested in the customer's stored electronic communications. It is only under these circumstances, or with a search warrant, that government agencies or officials are not required to notify electronic mail or remote computing services customers or subscribers that stored communications have been requested from the service provider.

Again, an electronic communications firm need only determine that a warrant or court order is facially valid in order to defend against suits for illegally disclosing communications to the government. In order to invoke this defense, however, a firm must have acted in good faith. Therefore, where a firm knows that an emergency situation does not in fact exist, it may be found to be acting in collusion with law enforcement officials and may be barred from asserting the good faith defense.

d. *Preclusion Of Notice*

Under the Electronic Communications Privacy Act, government agencies may also obtain a court order to prevent providers of electronic communications services or remote computing services from notifying anyone, including the customer or subscriber who is the subject of the investigation, that the agency has requested access to contents of or records about stored electronic communications.[29] Service providers are then required to comply with such court orders. Although the statute does not spell out penalties for noncompliance, as with other court orders, if the provider fails to comply, the provider could be cited for contempt of court.

A preclusion order may only be obtained in cases where the government is not required to notify the customer or subscriber, such as with a search warrant, or where the government has obtained the authority for delayed notification.[30] A court may grant such an order if there is reason to believe notification of the inquiry will lead to the adverse effects noted above.[31]

e. *When The Order Expires*

When the 90-day delayed notification order or certificate and all extensions granted under this provision expire, the investigating government agency must notify the customer or subscriber that the contents of the stored electronic communication have been disclosed. Such notification must be delivered by registered or first-class mail, or the notice must be served upon the customer or subscriber.[32]

At this point, it would be possible for the customer or subscriber to decide that an electronic mail or remote computing services provider, or the government, has violated the law against disclosure. The two-year statute of limitations on bringing a lawsuit against a service provider would begin at this point. However, it should be remembered that if the service provider disclosed any stored electronic communications in response to what appeared to be properly issued search warrants, court orders, or grand jury or administrative subpoenas, the provider may invoke the good faith reliance defense and would then be protected from such a suit.

The Act delineates specific information that must be included in the notification. The notification must state, in reasonably specific terms, the nature of the law enforcement inquiry.[33] It must also inform the customer or subscriber when the electronic communications service provided the information, that the notification was delayed, the authority under which the notification was delayed, and the provision of the Electronic Communications Privacy Act under which the government agency requested the information.[34]

C. The Standards For Customer Records And Other Information

1. Customer Lists And Other Information To Nongovernment Bodies

A provider of electronic mail or other electronic communications services may release information about customers or subscribers, but not the contents of their communications, to anyone but representatives of a government agency.[35] For example, in the course of normal business transactions, it is perfectly legal for an electronic mail or remote computing service provider to share customer transaction records as part of a sales pitch to increase usage of the system, or to sell customer lists.

2. Customer Lists And Other Information To Government Agencies

On the other hand, when government law enforcement officials seek access to customer or transactional records, rules similar to the 180-day rule for access to stored electronic mail messages apply. Electronic communications service providers may disclose customer lists and other information about customers or subscribers to government agencies or officials only if the government presents the proper authorizations to obtain such information.[36] Proper authorization would be one of the followin'

- Administrative subpoena authorized by federal or state statute or federal or state grand jury subpoena;[37]

- Warrant under Federal Rules of Criminal Procedure or the state equivalent;[38]

- Court order;[39] or

- Consent of the subscriber or customer.[40]

Should a government agency obtain customer records, but not the contents of customer communication, under the first three of the options above, the agency or official is **NOT** required to notify the customer or subscriber that such records have been obtained.[41]

Under these provisions, information about customers' or subscribers' usage of electronic communication systems, including billing and transactional records, and information about destination of communications, such as telephone toll records that include long distance phone numbers and message unit details, may be released.[42] Under no circumstances could contents of stored communications be released unless the order or subpoena specifically grants access to the contents.

D. Objecting To Disclosure

1. Contesting The Validity Of An Order

As noted above, in order to obtain authorization for access to 1) the contents of electronic communications stored more than 180 days, 2) transactional records about customers from an electronic mail firm, or 3) similar records from a remote computing service provider, the government agency or official must prove that it has reason to believe that the records or content sought are relevant to a legitimate law enforcement inquiry.[43] A service provider or customer may move to quash the court order and challenge the government's assertion that such reason exists. If such a challenge should prove successful, it would negate the order, warrant or subpoena, thus alleviating the service provider's responsibility to comply with the order.

2. Motion To Quash Or Modify Orders If Requests Are Unduly Burdensome

If the service provider feels a court order for information or records held by the provider is unusually voluminous or would cause undue burden on the provider, the provider may, in a timely fashion, make a motion to quash or modify the court order.[44] This provision has two purposes. First, it is intended to protect electronic mail and other electronic communications service providers from unduly burdensome requests.[45] Second, it grants the service provider access to an impartial judicial officer to determine whether the government's request is appropriate and properly focused.[46]

3. Customer Rights

As described above, the government must notify customers or subscribers of requests for contents or records of stored electronic communications in many instances. When such notice is required, it is primarily to give the customer an opportunity to object to the disclosure. The customer may do so with a variety of defenses, including constitutional claims under the First, Fourth, Fifth or Fourteenth Amendments.[47] If the customer objects, the court will likely order the service provider not to disclose the communication pending resolution of the customer's action.

When notice must be given to the customer or subscriber, the electronic mail or remote computing service provider is doubly protected from civil action for illegal disclosure of stored communications. First, the provider can rely in good faith on court orders and subpoenas provided by the government official or agency which requests disclosure. Second, when the customer is notified in advance, there is an opportunity for the customer to provide consent or authorization for the government to access the stored communications. Since either of these conditions provides a defense for the provider, the provider is doubly protected when the customer is notified in advance and does not object.

E. Defenses

1. Disclosure Under Court Order, Warrant Or Subpoena

The Electronic Communications Privacy Act prohibits litigation against any provider of electronic communications services, including employees of such firms, that provides information, facilities or assistance to government officials in accordance with the terms of a court order, warrant, subpoena or certification as specified in the law.[48] Should anyone bring suit against a service provider, the provider may defend itself with a good faith reliance on the government order presented which demanded disclosure of the information released.[49] (See Chapter 4 (E)(1) for further information on the good faith reliance defense.)

F. Covering The Costs Of A Government Request

1. Reimbursement For Direct Costs

The government is responsible for reimbursing electronic communication service providers for the direct costs involved in complying with a government request for information. The provider may charge for searching for, assembling, reproducing and performing other activities associated with providing the information. In addition, the provider is entitled to reimbursement for any necessary disruption of normal operations caused by the government's request.[50]

An electronic mail firm is not entitled to reimbursement for providing records or other information related to telephone toll records and listings.[51] These records are excluded because the government has long had access to telephone toll records without reimbursing telephone providers for access to those records.[52] This exception to the reimbursement rule is narrowly drawn and applies only to the provision of telephone toll records. For example, an electronic mail firm is entitled to compensation for telephone consultations providing technical advice to law enforcement officials, as well as for any court appearances made by the provider in connection with the information requested.[53]

Additionally, if such requests for telephone toll records are unusually voluminous or in some other fashion cause undue burden on the provider, a court may order the government to pay direct costs for receiving telephone records as well.[54] The legislative history notes that the basis for deciding if a request is unusually voluminous or unduly burdensome would be determined by an examination of past and current practices.[55]

2. Who Decides?

Payment required for direct costs of providing information to the government should be agreed upon between the government agency and the service provider.

Should the parties be unable to agree on an appropriate fee, the court which issued the order should decide the appropriate fee. If no court order was issued for the information provided, the fee would be determined by the court in which a criminal prosecution relating to the information was taking place.[56]

The House Committee noted in its report that it hoped the Department of Justice could devise a uniform set of standards that would reduce judicial intervention in decisions about cost reimbursement.[57]

1. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 68 (1986).
2. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All U.S. Attorneys and Strike Force Chiefs, December 15, 1986, 18.
3. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 68 (1986).
4. William Weld at 18.
5. William Weld at 18, 19.
6. Id.
7. 18 U.S.C.A. sec. 2703(a) (West Supp. 1988).
8. 18 U.S.C.A. sec. 2703(b)(1)(A) (West Supp. 1988).
9. 18 U.S.C.A. sec. 2703(b)(1)(B)(i) (West Supp. 1988).
10. 18 U.S.C.A. sec. 2703(b)(1)(B)(ii), 2703(d) (West Supp. 1988).
11. 18 U.S.C.A. sec. 2703(d) (West Supp. 1988).
12. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 68 (1986).
13. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 68, 69 (1986).
14. 18 U.S.C.A. sec. 2703(b)(2)(A) (West Supp. 1988).
15. 18 U.S.C.A. sec. 2703(b)(2)(B) (West Supp. 1988).
16. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All U.S. Attorneys and Strike Force Chiefs, December 15, 1986, 20.
17. William Weld at 20.
18. William Weld at 20.
19. William Weld at 20.
20. 18 U.S.C.A. sec. 2705(a)(1)(A) (West Supp. 1988).
21. 18 U.S.C.A. sec. 2705(a)(4) (West Supp. 1988).

22. 18 U.S.C.A. sec. 2705(a)(1)(B) (West Supp. 1988).

23. William Weld at 25.

24. 18 U.S.C.A. sec. 2705(a)(3) (West Supp. 1988).

25. 18 U.S.C.A. sec. 2705(a)(6) (West Supp. 1988).

26. William Weld at 25.

27. 18 U.S.C.A. sec. 2705(a)(4) (West Supp. 1988).

28. 18 U.S.C.A. sec. 2705(a)(2) (West Supp. 1988).

29. 18 U.S.C.A. sec. 2705(b) (West Supp. 1988).

30. William Weld at 26.

31. 18 U.S.C.A. sec. 2705(b) (West Supp. 1988).

32. 18 U.S.C.A. sec. 2705(a)(5) (West Supp. 1988).

33. 18 U.S.C.A. sec. 2705(a)(5)(A) (West Supp. 1988).

34. 18 U.S.C.A. sec. 2705(a)(5)(B) (West Supp. 1988).

35. 18 U.S.C.A. sec. 2703(c)(1)(A) (West Supp. 1988).

36. 18 U.S.C.A. sec. 2703(c)(1)(B) (West Supp. 1988).

37. 18 U.S.C.A. sec. 2703(c)(1)(B)(i) (West Supp. 1988).

38. 18 U.S.C.A. sec. 2703(c)(1)(B)(ii) (West Supp. 1988).

39. 18 U.S.C.A. sec. 2703(c)(1)(B)(iii) (West Supp. 1988).

40. 18 U.S.C.A. sec. 2703(c)(1)(B)(iv) (West Supp. 1988).

41. 18 U.S.C.A. sec. 2703(c)(2) (West Supp. 1988).

42. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 69 (1986).

43. 18 U.S.C.A. sec. 2703(d) (West Supp. 1988).

44. 18 U.S.C.A. sec. 2703(d) (West Supp. 1988).

45. S. Rep. No. 541, 99th Cong., 2nd Sess., 39 (1986).

46. S. Rep. No. 541, 99th Cong., 2nd Sess., 39 (1986).

47. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 69 (1986).

48. 18 U.S.C.A. sec. 2703(e) (West Supp. 1988).

49. 18 U.S.C.A. sec. 2707(d) (West Supp. 1988).

50. 18 U.S.C.A. sec. 2706(a) (West Supp. 1988).

51. 18 U.S.C.A. sec. 2706(c) (West Supp. 1988).

52. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 73 (1986).

53. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 74 (1986).

54. 18 U.S.C.A. sec. 2706(c) (West Supp. 1988).

55. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 74 (1986).

56. 18 U.S.C.A. sec. 2706(b) (West Supp. 1988).

57. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 74 (1986).

Chapter 6

When The Government Asks A Firm To Create Backup Files

A. Purpose

The Electronic Communications Privacy Act provides law enforcement officials with a valuable new tool to preserve evidence for criminal prosecutions. Under ECPA, if law enforcement officials believe that a criminal suspect may attempt to alter or destroy incriminating information in an electronic communications system, the authorities may direct an electronic mail firm to create duplicate copies of files in order to preserve them. This new provision will be especially helpful to authorities investigating financial crimes.

While the new rules requiring the creation of backup files might appear to impose added burdens on electronic mail firms, they also afford an important benefit. In effect, the creation of backup files under ECPA allows the government and the customer to fight out whether or not the government should eventually gain access to the backup files created, without involving an electronic mail firm in the dispute. The backup file rules protect a customer's right to contest the government's attempt to gain access to his or her electronic communications. And the creation of a backup file also satisfies the government's interest in preserving evidence.

This chapter will explain the procedures that law enforcement officials must follow in order to direct an electronic mail firm to create backup copies. In addition, this chapter discusses the steps that electronic mail firms must take in cooperating with the authorities. It is crucial that electronic mail executives and employees become familiar with the rules concerning the creation of backup files, because failure to comply with the rules can expose a firm to litigation.

In general, the new law allows government officials with valid court orders or subpoenas to **require** electronic mail firms to create backup copies without giving notice to the clients whose files are being duplicated. The theory underlying the law is that if notice is given, suspected criminals might attempt to alter files before copies could be created or might even attempt to interfere with the process of creating the copies. Although the government need not give notice to customers when the copies are made, before law enforcement authorities can **actually obtain** the copies, they are generally required to notify customers. The purpose of this provision is to use new technology to preserve evidence, not to make it easier for law enforcement officials to actually obtain it.

Electronic mail firms generally **must** create duplicate backup files when so directed by law enforcement officials. But, as this chapter explains, electronic mail firms, as well as their customers, may challenge government requests to turn over the backup files once created. Finally, this section discusses the procedures by which electronic mail firms can obtain reimbursement from law enforcement officials for the costs of providing assistance in creating backup files.

B. The Standards

1. Electronic Mail And Remote Computing Firms Must Create Copies

Government law enforcement officials may **require** electronic communications service providers, including electronic mail and remote computing firms, to create a backup copy of the contents of electronic communications in order to preserve the communications.[1] The purpose of this provision is to ensure that records of illegal activities will be preserved for use as evidence in criminal prosecutions.[2] Electronic mail and remote computing firms **must create** backup files when required to do so by law enforcement officials. There are other opportunities to challenge government requests when it is time to actually turn over the copies made.

2. Electronic Mail And Remote Computing Firms Should Only Create Copies When Law Enforcement Officials Present Them With A Court Order Or Subpoena

Law enforcement officers must include a demand to make backup copies in a request for a court order or subpoena.[3] Electronic mail and remote computing firms should ask law enforcement officials for a copy of a court order or subpoena before making the backup copies. Electronic mail and remote computing firms cannot be sued nor can their officers, employees or agents be sued for providing assistance in accordance with the terms of a court order or warrant.[4]

As is the case of cooperating with government efforts to intercept electronic mail in transmission or in obtaining the contents of an electronic mail message, electronic mail firms have a positive **duty** to read court orders requesting the creation of duplicate backup copies. If representatives of a firm do not read a court order, the firm cannot defend itself in a suit by an aggrieved customer by claiming that firm relied "in good faith" on a court order. The duty to read the court order does not require that a firm legally analyze the validity of the order, only that a representative of the firm read the court order and that it appeared to be valid.

Similarly, an electronic mail firm must only cooperate with law enforcement officials within the scope of a court order. Therefore, duplicate backup copies should be made only of those files specified in the court order and no other files. If the backup tapes are turned over to government officials, disclosing records outside the scope of the court order may prevent an electronic mail firm from invoking the good faith defense and may subject a firm to liability. (See Chapter 4 (E)(1) regarding the good faith defense.)

3. *Electronic Mail And Remote Computing Firms Must Not Notify Customers That A Court Order Or Subpoena Has Been Issued Requiring Copies To Be Made*

ECPA specifically states that electronic mail and remote computing firms **must not** notify customers that a court order or subpoena has been issued requiring the creation of backup files.[5] This directive should also be construed as prohibiting electronic mail and remote computing firms from notifying their customers that they are making backup copies of their records. While this section of the law does not set out a specific penalty for informing customers of the request to create backup copies, the legislative history for other similar provisions in the law suggests that a firm that informs a client that copies are made may be liable for criminal contempt.[6]

4. *Electronic Mail And Remote Computing Firms Must Create Backup Copies As Soon As Practicable, But In No More Than Two Business Days*

An electronic mail or remote computing firm must create backup files requested by law enforcement officials "as soon as practicable consistent with its regular business practices" after being served with a court order or subpoena.[7] Therefore, if a firm maintains backup copies as part of its regular business activities, the firm does not have to create an entirely new copy.[8] Whether or not a firm has to create an entirely new copy, there must be a copy no later than two business days after the firm was served with a court order or subpoena.[9]

Therefore, if a firm can create a backup file in less than two business days without creating an undue burden on its employees or causing interference with the service the firm provides to its customers, it should do so. If this is not possible, the firm has a legal obligation to create the file by the end of business on the second day after the firm is served with a court order or subpoena. Again, no specific penalty for failure to comply is provided, but other sections of the law suggest that a firm may be held in contempt for failure to create the backup files within the two-day limit.

5. *Electronic Mail And Remote Computing Firms Must Confirm To Law Enforcement Officials That A Copy Has Been Made*

After the backup copy has been made, an electronic mail and/or remote computing firm **must** confirm to the law enforcement agency serving the court order or subpoena that the backup copy has been made.[10] It is unclear whether this confirmation need be in writing. The legislative history of ECPA only suggests that a firm must "inform" law enforcement officials that the firm has complied with the request to make a copy.[11]

It is advisable, however, for a firm to confirm the creation of a duplicate backup file in writing in order to document cooperation with law enforcement officials.

6. *After A Firm Confirms That A Backup File Has Been Created, Law Enforcement Officials Must Generally Notify Customers That The Copy Has Been Made*

Within three days after an electronic mail or remote computing firm confirms to law enforcement officials that a backup file has been created, the government is required in most cases to notify a customer that backup copies of his or her files have been made.[12]

Unless notice by the government is delayed (as described below), an electronic mail or remote computing firm is also free to notify a customer that his or her files have been copied once the routine, three-day deadline for notice by the government has expired.[13] Before providing notice to customers, however, it would be wise to first double-check with law enforcement officials to ensure that notice is not being delayed by the government.

If certain tests are met, law enforcement officials may delay notice to customers that 1) the government is seeking to obtain copies of their communications; and 2) the government has requested that an electronic mail firm create a backup file. (See discussion of these factors in Chapter 5.)

7. *Electronic Mail And Remote Computing Firms Must Not Destroy Backup Copies Until Certain Conditions Are Met*

Electronic mail and remote computing firms may not destroy backup files created pursuant to a request from law enforcement officials until the information sought by authorities has been delivered, or any legal challenge to a court order or subpoena requiring copying has been completely resolved.[14]

A legal challenge to a court order or subpoena is considered to be completely resolved for purposes of this rule when all appeals have been exhausted.

8. *Electronic Mail And Remote Computing Firms Generally Must Turn Over Backup Copies To Law Enforcement Officials No Sooner Than 14 Days After The Government Notifies A Customer That His Or Her Files Have Been Copied*

No sooner than 14 days after law enforcement officers notify a customer that his or her files have been copied, an electronic mail or remote computing firm must generally turn over the copies to law enforcement officials.[15] This 14-day period gives a customer adequate time to contest the government's request.

First, if a firm has not received written notice from a customer that he or she is challenging the government's request within the 14-day period, the firm must generally turn over the copied files to law enforcement officials.[16]

Second, an electronic mail or remote computing firm need not turn over the backup files to government officials if, within the 14-day period, the firm itself has initiated a legal challenge to the government request.[17]

C. Challenges By Electronic Mail And Remote Computing Firms

An electronic mail or remote computing firm has 14 days after law enforcement agents notify a customer that a backup file has been created to itself initiate a challenge to the court order requiring the creation and disclosure of the backup copy.[18] A provider may challenge a court order by claiming that the backup copies sought are not relevant to a legitimate law enforcement inquiry.[19]

Further, a firm may move to quash or modify a court order if the information requested is unusually voluminous or if compliance with the order would create an undue burden on the firm.[20] Communications service providers are given this special standing in order to protect electronic mail firms and others from unduly burdensome requests and to give an impartial judge an opportunity to evaluate the government's request.[21]

If a firm is going to challenge a court order because compliance with the order would be unduly burdensome or would interfere with the service provided by an electronic mail firm, the firm should be prepared to support its contention with evidence. The firm should demonstrate, for example, that the amount of computer time required to copy extraordinarily voluminous files would prevent customers from using the system or severely slow down and interfere with the system. A firm might also argue that it does not have a sufficient number of employees to properly manage the system while providing the extraordinary amount of assistance required by law enforcement officials. A firm should **not** argue, however, that the financial costs of creating duplicate backup files is too great, because the law requires law enforcement officials to compensate electronic mail firms for costs incurred in creating backup files.

Neither an electronic service provider nor a customer may challenge the decision by government officials to delay notice of the creation of backup files.[22] The decision to delay notice is left to the sole discretion of law enforcement officials, if the officials determine that the existence of a court order might alert suspected criminals and result in the destruction of or tampering with files.[23] Backup files are maintained solely to ensure that evidence will not be tampered with or destroyed. Keeping the mere creation of the file secret does not interfere with a customer's privacy interest; that interest might only be harmed when the files are actually turned over to government officials.[24]

D. Challenges By Customers

1. *Grounds For A Customer Challenge*

A customer must file a sworn affidavit that he or she is a customer of the electronic mail or remote computing service that law enforcement officials have asked to make a backup file and that the files sought are his or hers.[25] In other words, the customer must establish that he or she is the "relevant" customer for purposes of making such a challenge.[26]

A customer must also show 1) that the records sought are not relevant to a legitimate law enforcement inquiry; 2) that law enforcement officials have not substantially complied with any other provisions of ECPA;[27] or 3) that there is some other legal defect in the court order or subpoena.[28]

2. *Legal Procedures For Customer Challenges*

A customer must file a motion to quash a subpoena or vacate a court order within fourteen days of receiving notice from law enforcement officials that copies of his or her records are being sought.[29] Copies of the motion must be served on the law enforcement officials who applied for the original order, and a customer must provide written notice of the challenge to the electronic mail or remote computing firm.[30] When an electronic mail firm receives such a notice, it must **not** turn over the duplicate backup copies it has created until the challenge is resolved and a court directs the firm to turn over the files.

A motion to quash a subpoena must be filed in the appropriate federal district court or state court.[31]

Special rules of service of process are set out for customer challenges. Most notably, a customer challenging a subpoena or court order is directed to serve the person, office or department specified in the notice received from law enforcement officials stating that the government is seeking copies of the customer's records.[32]

Congress intended that judicial decisions on customer challenges should occur as rapidly as possible, within seven calendar days in all but the most unusual circumstances.[33]

3. *Procedures Governing The Response Of Law Enforcement Officials To A Challenge*

If a customer challenging an order to create a backup copy meets the procedural requirements of the new law (i.e., meets deadlines, notice and pleading requirements), law enforcement officials must file a sworn response to the challenge with the court.[34]

The response may be filed in a closed-door, in-camera proceeding if appropriate (for example, if an open hearing would compromise a law enforcement investigation or pose a threat to life).[35] A court may order additional proceedings if its initial review of the customer's challenge and the government's response does not dispose of the motion.[36] Rulings on challenges to court-ordered backup duplication are not subject to interlocutory appeal and, therefore, must await a final decision in the entire case to be appealed.[37]

E. Who Pays When The Government Requests Duplicate Backup Files?

1. Government To Reimburse Direct Costs

When law enforcement officials require an electronic mail or remote computing firm to create duplicate backup files, ECPA requires law enforcement agencies to reimburse firms for "reasonably necessary" costs which have been **directly incurred** in searching for, assembling, reproducing or otherwise providing such information. The costs to be reimbursed include costs resulting from the **necessary** disruption of normal operations of an electronic mail or remote computing service.[38]

Therefore, electronic mail firms should carefully keep track of the hours that employees must devote to creating backup files, and bill law enforcement officials at the normal hourly rate for such work. In addition, electronic mail firms should measure the amount of computer time required to create the backup files and bill the government at the normal rate for computer use. Further, if an electronic mail firm incurs costs because service to customers is interrupted, it may attempt to collect from the government the amount of revenue which the firm would normally receive during the period of the disruption. Finally, an electronic mail firm should be compensated for any costs associated with restoring service after an interruption caused by creating duplicate backup copies.

2. Exact Amount Of Reimbursement To Be Mutually Agreed Upon

Based on the above criteria, the exact amount of reimbursement due an electronic mail or remote computing firm is to be mutually agreed upon by the firm and law enforcement officials.[39] If no agreement can be reached, a court is empowered to set a "reasonable" fee.[40] The court which issued the court order directing that copies be made will normally resolve most disputes. In those cases where no court order was issued, the court hearing the criminal prosecution may set the fee.[41]

As is the case with disputes concerning reimbursement for the costs of assisting official interceptions of electronic mail, a firm should carefully consider the financial costs of litigating a dispute with law enforcement officials concerning the amount of reimbursement due.

1. 18 U.S.C.A. sec. 2704(a)(1) (West Supp. 1988).
2. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 70 (1986).
3. 18 U.S.C.A. sec. 2704(a)(1) (West Supp. 1988).
4. 18 U.S.C.A. sec. 2703(e) (West Supp. 1988).
5. 18 U.S.C.A. sec. 2704(a)(1) (West Supp. 1988).
6. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 77 (1986).
7. 18 U.S.C.A. sec. 2704(a)(1) (West Supp. 1988).
8. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 70 (1986).
9. 18 U.S.C.A. sec. 2704(a)(1) (West Supp. 1988).
10. 18 U.S.C.A. sec. 2704(a)(1) (West Supp. 1988).
11. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 70 (1986).
12. 18 U.S.C.A. sec. 2704(a)(2) (West Supp. 1988).
13. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 70 (1986).
14. 18 U.S.C.A. sec. 2704(a)(3) (West Supp. 1988).
15. 18 U.S.C.A. sec. 2704(a)(4) (West Supp. 1988).
16. S. Rep. No. 541, 99th Cong., 2nd Sess., 41 (1986).
17. 18 U.S.C.A. sec. 2704(a)(4)(B) (West Supp. 1988).
18. 18 U.S.C.A. sec. 2704(a)(4)(B) (West Supp. 1988).
19. 18 U.S.C.A. sec. 2703(d) (West Supp. 1988).
20. Id.
21. S. Rep. No. 541, 99th Cong., 2nd Sess., 39 (1986).
22. S. Rep. No. 541, 99th Cong., 2nd Sess., 40 (1986).

23. 18 U.S.C.A. sec. 2704(a)(5) (West Supp. 1988).

24. S. Rep. No. 541, 99th Cong., 2nd Sess., 40 (1986).

25. 18 U.S.C.A. sec. 2704(b)(1)(A) (West Supp. 1988).

26. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 70 (1986).

27. 18 U.S.C.A. sec. 2704(b)(1)(B) (West Supp. 1988).

28. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 70 (1986).

29. 18 U.S.C.A. sec. 2704(b)(1) (West Supp. 1988).

30. Id.

31. Id.

32. 18 U.S.C.A. sec. 2704(b)(2) (West Supp. 1988).

33. H. R. Rep. No. 647, 99th Cong., 2nd Sess., 71 (1986).

34. 18 U.S.C.A. sec. 2704(b)(3) (West Supp. 1988).

35. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All States Attorneys and Strike Force Chiefs, December 15, 1986, 24.

36. 18 U.S.C.A. sec. 2704(b)(3) (West Supp. 1988).

37. 18 U.S.C.A. sec. 2704(b)(5) (West Supp. 1988).

38. 18 U.S.C.A. sec. 2706(a) (West Supp. 1988).

39. 18 U.S.C.A. sec. 2706(b) (West Supp. 1988).

40. S. Rep. No. 541, 99th Cong., 2nd Sess., 43 (1986).

41. 18 U.S.C.A. sec. 2706(c) (West Supp. 1988).

Chapter 7 Pen Registers And Trap And Trace Devices

A. Purpose

Title III of the Electronic Communications Privacy Act regulates the use of pen registers and trap and trace devices, devices used by law enforcement agencies and communications providers to determine the destination of an outgoing phone call or electronic transmission and the origin of incoming calls or transmissions.

ECPA generally prohibits the use of these communications tracking devices, thus preventing individuals, creditors, government agencies and others from determining with whom another individual is communicating, and thereby protecting the privacy of telephone customers and electronic mail users. Important exceptions to the general prohibition against use of these devices, however, allow electronic mail and other communications firms to use pen registers and trap and trace devices to record the initiation and completion of phone calls and electronic communications for billing purposes, to track down individuals who use a communications system fraudulently, and where the consent of the user has been obtained.[1]

Another important exception is provided for the use of pen registers and trap and trace devices by authorized law enforcement officers as part of criminal investigations.[2] The new law sets out procedures under which law enforcement officers must generall obtain warrants, subpoenas or court orders in order to track the origin and destinatio of communications via these technologies. This chapter will explain the rights and duties of electronic mail firms when law enforcement officials ask for assistance in installing and monitoring pen registers and trap and trace devices. The responsibilities of electronic mail firms under ECPA are similar, if not identical, to those imposed on telephone companies ranging in size from small rural telephone cooperatives to large regional operating companies.

Prior to enactment of the new pen register and trap and trace provisions, the U.S. Supreme Court held that law enforcement officials need not obtain a search warrant in order to gain assistance from a telephone company or other communications provider in installing a pen register.[3] The Court reasoned that an individual who uses a telephone voluntarily discloses the numbers he or she dials (i.e., for billing purposes) and has "no reasonable expectation of privacy" and, therefore, the Fourth Amendment to the Constitution does not limit the use of pen registers.[4]

In response to concerns from phone companies about civil liability for disclosing information to law enforcement officials derived from these tracking devices, the Justice Department until 1986 voluntarily adopted a policy of requiring court orders for the use of pen registers and trap and trace devices.[5] According to one of the sponsors of ECPA, while this voluntary policy was welcome, the Supreme Court's decisions an federal statutes "left federal law enforcement officials with virtually unchecke discretion to obtain information through the use of pen registers."[6]

Therefore, Title III of ECPA generally codifies the Justice Department's practice of requiring court orders for use of pen registers and trap and trace devices by law enforcement officials.[7] The new law also sets out procedures for obtaining court orders and establishes guidelines for cooperation by communications providers with law enforcement officials. The law clarifies that the use of pen registers by private individuals without a court order is illegal except when the individual is an employee of a communications firm which is using these devices for permissible purposes such as accounting.

In 1988, Congress made a substantial addition to the original pen register and trap and trace provisions enacted in 1986. The new provisions create guidelines for obtaining authorization to install these devices in certain emergency situations, including when an individual's life is in danger and there is little or no time to apply for a court order authorizing use of a pen register or trap and trace mechanism.

B. The Standard: Pen Registers And Trap And Trace Devices Require Court Order

1. *The Standard Generally*

No person may install or use a pen register or a trap and trace device without a court order, subject to the exceptions (including an exception for electronic mail firms that use these devices for billing and accounting) outlined below.[8] This provision alters the Supreme Court's decision in *Smith v. Maryland,* which held that the Fourth Amendment to the Constitution did not limit the use of pen registers nor require law enforcement officials to obtain court orders for their use.[9]

2. *Definitions: Which Devices Are Regulated By The Act?*

ECPA provides expansive definitions of pen registers and trap and trace devices which include the mechanical devices specifically known by these names and other technologies which perform similar functions.[10] Whether or not the devices an electronic mail firm uses to record communications are governed by the new law may depend on whether or not these devices fall within the statutory definitions.

a. *Pen Registers*

A "pen register" is defined as a device which "records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached."[11] As the legislative history suggests, pen registers record only the telephone numbers "dialed out" of a phone line and do not record the contents of communications.[12] A plain reading of the statute and legislative history suggests that the definition of pen registers, for purposes of the prohibition on their use, is limited to devices used in conjunction with a telephone line. Therefore, a device recording outgoing communications over an internal electronic mail system that functions through a central processing unit without telephone lines would not be regulated by the new law. A similar device used on an electronic mail system that functions over phone lines would be regulated by the Act, subject to the following exceptions.

The definition of "pen register" specifically **excludes** certain types of equipment and certain uses. Any device used by an electronic mail or communications firm or its customers for recording communications in order to bill customers is excluded from the definition and regulation under the Act.[13] Devices used for cost accounting by electronic mail and other communications firms or their customers are also excluded.[14] Therefore, electronic mail firms may continue to use pen registers and trap and trace devices for billing and accounting without being subject to the new restrictions.

In addition, the legislative history clearly states that devices used by some firms to record billable time for their clients' accounts are not prohibited by the Act.[15] Thus, the devices used by many law firms to record the length of telephone calls for billing purposes are not subject to the Act. Neither does the law regulate devices used to account for computer usage attributable to a client.

b. *Trap And Trace Devices*

ECPA defines "trap and trace devices" as devices which capture incoming electronic or other impulses which identify the originating number of **an instrument or device** from which a wire or electronic communication was transmitted.[16] Thus, while the definition of "pen registers" apparently is limited to devices used in conjunction with telephones, the use of trap and trace devices is regulated by ECPA regardless of whether these mechanisms are used in conjunction with a telephone line. Therefore, devices that monitor incoming communications and can identify their origin[17] are regulated by the Act regardless of whether the communication travels over an external phone line or an internal computer network. These devices are particularly valuable to electronic mail and other electronic communications providers in tracking down hackers and others who break into systems. No exclusions are provided in the definition of trap and trace devices.

Thus, trap and trace devices used by **all** electronic mail firms, regardless of whether the service is connected by telephone lines, may be regulated by the new act. Whether or not the new rules apply to a specific firm will depend on whether or not the firm uses trap and trace devices in a manner excluded from regulation by the following statutory exceptions.

C. The Exceptions

While ECPA generally prohibits the use of pen registers and trap and trace devices by any party that does not have a valid court order, the new law sets out certain practical exceptions to allow electronic mail firms, telephone companies and other communications providers to monitor the flow of communications on their systems.

1. To Operate, Maintain And Protect Electronic Mail Systems

An electronic mail firm or other wire or electronic communication service may use pen registers and trap and trace devices to operate, maintain and test their service.[18] In addition, these devices may be used to protect the rights or property of the firm and to protect customers from abuse of the service or unlawful use of the service.[19] For example, trap and trace devices may be used by electronic communications firms to identify the telephone numbers of computer hackers or other intruders who threaten harm to communications systems. This exception will provide some relief to electronic communications firms that have encountered difficulty in enlisting the support of telephone companies and law enforcement officials in tracking down intruders. Overburdened law enforcement officials, for example, may be reluctant to assign investigators to a computer crime case unless an electronic mail firm performs much of the technical groundwork needed to locate intruders. This exception will permit electronic mail firms to install trap and trace devices to identify the location of intruders and then turn that information over to law enforcement authorities to aid their own investigations. In addition, pen registers are an effective means of detecting illegal communications pirating devices, such as so-called "blue boxes,"[20] and when used for this purpose are not prohibited by the Act.

2. To Record The Beginning And End Of Messages For Billing And Accounting

Electronic mail and other communications firms may use pen registers and trap and trace devices to record the initiation and completion of communications, including electronic mail messages, in order to protect themselves or other firms involved in forwarding the message.[21] In addition, these devices may be used to record the initiation and completion of communications to protect customers from fraud, unlawful use of an electronic mail service or abuse.[22] For example, telephone companies use pen registers to verify billing information,[23] and also use these devices to track down obscene phone callers.[24] Many electronic mail firms make the same use of these devices for billing and accounting. Congress did not intend to prohibit such uses of pen registers and trap and trace devices.

3. Consent

Finally, a telephone company or electronic communications firm may install pen registers and trap and trace devices "where the consent of the user of that service has been obtained."[25] While this provision would appear to be relatively straightforward, a controversy is developing about whether or not this provision allows the use of so-called "caller identification" systems for telephones. Although this debate largely concerns telephone companies, electronic mail firms may be interested in the controversy.

Caller identification systems allow a telephone customer to view the telephone number of an incoming call on a small digital display screen attached to the telephone. Questions have been raised about whether these devices violate the privacy of callers placing calls without the knowledge that their phone number is being identified by the recipient of the call. Specifically, all parties agree that caller identification systems clearly fall within the definition of trap and trace devices, because they identify the origin of an incoming call.

Proponents of caller identification systems argue that although these devices fall within the definition of trap and trace devices, they are legal because individuals who use caller identification equipment have consented to the installation of such devices Opponents argue that the language of ECPA specifically limits the consent exception to an installation by a provider where the consent of the user has been obtained rather than as a general authorization of caller identification systems. Some state public utility commissions that have reviewed the legal question have concluded that the consent language in the statute is sufficient to authorize caller identification systems. Recently, however, a Pennsylvania court ruled that the language of the Pennsylvania state statutute, which mirrors ECPA, prohibited the use of a caller I.D. system in that state. (*Barash v. Pennsylvania Public Utility Commission,* Commonwealth Court of Pa., No 2270, May 30, 1990) Bills have been introduced in both Houses of Congress that, if enacted, would require service providers to provide callers with the ability to block the transmission of the telephone number from which the call is being made. California has implemented this policy through legislation.

D. The Penalties

Knowing violations of the prohibition against the use of pen registers and trap and trace devices are punishable by up to one year in prison or fines of up to $250,000 for individuals and $500,000 for organizations, or both.[26]

E. The Procedures For Obtaining A Court Order

Although the procedures for obtaining a court order authorizing the use of pen registers and trap and trace devices apply solely to law enforcement officials, electronic mail firms and users should become familiar with the rules because a firm must not cooperate with authorities if it is aware that law enforcement officials have violated these procedures.

For a federal criminal investigation, an attorney for the government must apply for a court order authorizing the use of pen registers and trap and trace devices.[27] For state criminal investigations, the new law only requires that a state investigative or law enforcement officer, as opposed to an attorney, make the application.[28]

In either case, the application for a court order must be sworn and in writing and submitted to a court of competent jurisdiction.[29]

The application must identify the attorney for the federal government or state law enforcement official seeking the court order and must also identify the law enforcement agency conducting the criminal investigation.[30] The application must certify that the information likely to be obtained by using pen registers and trap and trace devices is **relevant to an ongoing criminal investigation.**[31] This is a lesser standard of proof than probable cause or reasonable suspicion, and the Justice Department maintains that this language was included because individuals do not have a reasonable expectation of privacy in the numbers dialed to and from a telephone.[32]

It is important to note, however, that ECPA specifically states that the new law does not preempt state laws governing the use of pen registers and trap and trace devices.[33] Where states maintain higher standards of proof, the state law applies to state court orders. In addition, where state law specifically designates which law enforcement officials or state attorneys may apply for court orders, state law applies.[34] Therefore, it is important for an electronic mail firm to become aware of the pen register and trap and trace laws in the states where it is located and conducts business.

F. The Court Order, Its Duration, And Restrictions On Electronic Mail Firms In Disclosing Existence Of Devices

An electronic mail or communications firm cannot be sued for cooperating with law enforcement officials if assistance, facilities or information are provided in accordance with a court order.[35]

In order to avoid a lawsuit, however, a firm must read a court order and determine that it is facially valid. In addition, the firm must only provide assistance to law enforcement officials within the scope of the court order. Therefore, it is important that electronic mail firms gain some knowledge of the procedures outlined below.

1. The Standard For Issuing Court Orders

A court of competent jurisdiction is directed by the new law to issue an ex parte order (without an opportunity for the criminal suspect to be heard) if an attorney for the federal government or the relevant state law enforcement official certifies that the information likely to be obtained by use of a pen register or trap and trace device is **relevant to an ongoing criminal investigation.**[36]

A court of competent jurisdiction in federal cases refers to any district court of the United States. Federal magistrates may issue such orders.[37]

There is a discrepancy in the legislative history concerning the extent to which a judge is to review the applicant's certification that use of these devices is relevant to a criminal investigation. The Senate Committee Report states that "to issue an order, the court must first be satisfied that the information sought is relevant to an ongoing criminal investigation."[38] The House Committee Report suggests a less rigorous standard of review under which a judge shall issue an order if the court simply finds that a government attorney has certified to the court that the information sought is likely to be relevant.[39]

The Senate Committee Report explains, however, that "this provision does not envision an independent judicial review of whether the application meets the relevance standard, rather, the court needs only to review the completeness of the certificatior submitted."[40] This apparent discrepancy in the Senate report language may give judges some leeway to review the relevance to criminal investigations of requests to use pen registers and trap and trace devices. The Department of Justice does not share this view, however, maintaining that a court "need only review the completeness of the attorney's certification."[41] The Department claims that there is no need for government attorneys to substantiate their requests for court orders with factual affidavits, but only for government attorneys to provide a sworn application with the requisite certification along with a draft order.[42]

2. Contents Of Court Orders

A court order authorizing the use of pen registers and trap and trace devices must specify the name of the person who leases the telephone to be monitored by the devices or in whose name it is listed.[43] The court order must also give the name of the person who is the subject of the criminal investigation, if his or her identify is known.[44] In addition, the order must specify the number and physical location of the telephone lines to which the devices are to be attached.[45] In other words, a court order should specifically identify the location of the **particular facility** maintained by an electronic mail or communications firm. When trap and trace devices are used, a court order must specify the geographic limits of the order, rather than identify the specific facility.[46] Finally, the court order must state the offense to which the information sought by us of the devices relates.[47]

3. Court Order Must Contain Directive To Firms To Cooperate

If law enforcement officials request assistance from communications firms in installing and using pen registers and trap and trace devices, a court order must direct that a firm furnish information, facilities and technical assistance necessary to install the device.[48] This provision of court orders codifies the former practice of the Justice Department in cooperating with telephone companies.[49] The requirement that a court order specifically direct an electronic mail or communications firm to provide assistance to law enforcement officials will help firms defend against lawsuits by aggrieved customers by helping document that the firms acted in good faith reliance on court orders.

Electronic mail and communications firms should provide no more assistance than they are directed to by a court order. While court orders are not likely to specify the step-by-step assistance to be provided, firms should be careful only to provide assistance **necessary** to install and/or monitor the device. Providing assistance beyond what is necessary, such as suggesting to law enforcement officials that they may wish to monitor communications other than those specified in the court order, may constitute collusion with authorities and expose a firm to a civil suit.

4. Electronic Mail Firms May Not Disclose The Existence Of Devices

When a court order is issued authorizing the use of pen registers and trap and trace devices, ECPA provides that the order contain specific provisions **forbidding** electronic mail firms and others from disclosing the existence of these devices to anyone, including customers, unless the court otherwise directs.[50] Specifically, the order will prohibit the owner or lessor of the phone line that is being monitored or the firm providing assistance to law enforcement officials from disclosing the existence of pen registers and trap and trace devices.[51]

Individuals or firms that intentionally violate a court order prohibiting disclosure of the existence of pen registers and trap and trace devices may be punished for contempt in appropriate circumstances.[52]

The basic rule is that electronic mail firms and their employees **must not** tell anyone, including customers or family members, that a pen register or trap and trace device has been installed. Failure to follow this rule could result in a prison term.

Finally, unless a judge rules otherwise, a court order authorizing the use of pen registers and trap and trace devices must be sealed, presumably to prevent tipping off criminal suspects of an investigation.[53]

5. The Duration Of Court Orders

Law enforcement officials may use pen registers and trap and trace devices for up to 60 days when authorized by a court order.[54] Extensions of up to 60 days may be granted.[55] This is a doubling of the 30-day period for extensions previously observed by the Justice Department. The Department suggests that this extended period will reduce the need for multiple extensions.[56] Electronic mail and communications firms should not provide assistance to law enforcement officials beyond the period specified in the court order or extension. Providing assistance beyond this time period may expose a firm to civil liability.

G. Assistance With Installation Of Pen Registers And Trap And Trace Devices

1. Assistance Required In Installing Pen Registers

Providers of wire and electronic communication services, landlords, custodians and other persons must provide government officials or attorneys with all the information, facilities and technical assistance necessary to install a pen register unobtrusively and with minimal service interference, as long as the officials or attorneys have obtained a proper court order, as described above.[57] As is current practice, it is expected that law enforcement officials will install and maintain the pen register.[58]

Therefore, if law enforcement officials present a court order, and representatives of the firm **read** the court order and are **not aware** of any improper activity on the part of the authorities, an electronic mail firm and its employees must provide

- Access to facilities;

- Technical advice and assistance in installing a pen register (but the law enforcement officials must perform the actual installation); and

- Technical advice and assistance in maintaining the pen register (but law enforcement officials must do the majority of the work in maintaining the pen register).

2. Assistance Required In Installing And Maintaining Trap And Trace Devices

Providers of wire and electronic communication services, landlords, custodians and other persons must promptly install a trap and trace device on the appropriate line when presented with an order to do so.[59] In addition, electronic mail and communications firms are responsible for monitoring information collected by trap and trace devices. In this case, unlike the case with pen registers, **service providers will generally install** the devices themselves.[60] The provider must also furnish government officials or investigating authorities with additional pertinent information, facilities and technical assistance to install the device unobtrusively and with a minimum of service interference.[61]

Electronic mail and communications firms must provide information from a trap and trace device to the government official requesting the information at reasonable intervals during regular business hours for the duration of the court order, unless otherwise specified in the order.[62] The Department of Justice and telephone companies have agreed that the following technical language be included in applications for technical assistance involving trap and trace devices:

- The tracing operation must be limited to Electronic Switching Systems or No. 5 cross bar facilities;

- The tracing operation is to be restricted to tracing and recording only calls originating from a specific city within a certain radius or, in large cities, from specific sections of the city; and

- The tracing operation is to be restricted to certain specific hours of the day.[63]

3. Electronic Mail Firms To Be Compensated For Assistance

The Electronic Communications Privacy Act requires the government to reasonably compensate electronic mail and communications firms that furnish information or assistance relating to pen registers or trap and trace devices for the expenses incurred in providing such assistance.[64] This language is designed to permit maximum flexibility in compensating providers for the assistance they provide, and to make the reimbursement appropriate to the amount of work required in carrying out the order.[65]

Therefore, firms should carefully keep track of the number of hours employees must devote to assisting law enforcement officials and in monitoring trap and trace devices and should bill the government for the normal hourly rate. In addition, the government should be billed for any computer time required.

Finally, while this section of the law does not provide a mechanism to resolve disputes with the government concerning the amount of compensation due, a good faith argument can be made that the dispute resolution mechanism set out in other parts of the new law should apply. Specifically, if an electronic mail firm cannot reach agreement with law enforcement officials concerning compensation, the firm should ask the court which issued the court order to settle the dispute by determining a reasonable amount of compensation.[66]

4. *Firms Are Immune From Suits When Cooperating With Court Orders*

Electronic mail and communications firms, and their employees and agents, cannot be sued when they have provided information or assistance in accordance with the terms of a court order.[67] In addition, a good faith reliance on a court order, legislative authorization or statutory authorization is considered a complete defense against any civil or criminal action brought under this or any other law.[68]

Once again, in order to avoid a lawsuit and invoke the good faith defense, a firm representative **must read** a court order. In addition, the firm must only offer assistance to law enforcement officials within the scope of the court order. Finally, a firm must not cooperate with law enforcement officials if the firm is aware that the authorities have acted improperly, e.g., if the firm was informed that the police did not obtain a court order that is **actually** valid. In short, a firm need not perform a legal analysis of a court order, but if a firm is aware that a court order is not valid, the firm should not cooperate with authorities until it is convinced that the court order is valid.

H. New Amendment To ECPA Concerning Emergency Installation

In 1988 Congress passed a series of relatively minor changes to the Electronic Communications Privacy Act. Most important among these changes were provisions allowing law enforcement authorities to install pen registers and trap and trace devices in those emergency situations where there is little or no time to apply for a court order.

Under the new ECPA amendments, appropriate investigative or law enforcement officials of the state or federal government may request emergency installation of either pen registers or trap and trace devices, if they comply with certain requirements. First, they must reasonably determine that an emergency situation exists and that the installation must occur before a court order can be obtained.[69] Emergency situations include

- Immediate danger of death or serious bodily injury to any person; and

- Conspiratorial activities characteristic of organized crime.[70]

Second, the authorities must, within 48 hours of the installation of the device, obtain the appropriate court order authorizing installation and use of the device.[71] If an order is not obtained, use of the device must terminate the first time one of the following conditions occurs:

- The information sought is obtained;

• The application for the order is denied; or

• Forty-eight hours have lapsed since the installation of the device.[72]

Law enforcement officials must receive authorization from top Justice Department officials or high-level state prosecutors to invoke emergency installation of trap and trace or pen register devices. Specifically, the officials must be designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, any Deputy Assistant Attorney General, or the principal prosecuting attorney of any state or subdivision thereof in accordance with state statutes.[73]

Any investigative or law enforcement official who installs or uses a trap and trace device or pen register on an emergency basis but does not apply for the appropriate authorizing order within 48 hours will have violated the Electronic Communications Privacy Act.[74]

In order to protect itself from litigation, an electronic mail firm **should not** provide assistance to law enforcement officials when they claim that an emergency situation exists, unless the officials can confirm, preferably in writing, that they have received high-level authorization to install the pen register and trap and trace devices without a court order in hand. If the officials will not provide any assurance in writing, a firm should ask for the name of the high-level attorney who authorized the emergency installation and attempt to contact that individual before cooperating.

Electronic mail and communications firms that assist in the emergency installation of trap and trace devices or pen registers are entitled to reasonable compensation for expenses incurred during such assistance.[75]

1. 18 U.S.C.A. sec. 3121(b) (West Supp. 1988).

2. Id.

3. *Smith v. Maryland*, 442 U.S. 735, 746 (1979).

4. Id.

5. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All States Attorneys and Strike Force Chiefs, December 15, 1986, 29.

6. Congressman Robert W. Kastenmeier, Deborah Leavy and David Beier, "Communications Privacy: A Legislative Perspective," 4 Wis. L Rev. 715, 731 (1989).

7. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All States Attorneys and Strike Force Chiefs, December 15, 1986, 29.

8. 18 U.S.C.A. sec. 3121(a) (West Supp. 1988).

9. *Smith v. Maryland*, 442 U.S. 735 (1979).

10. 18 U.S.C.A. sec. 3126(3), (4) (West Supp. 1988).

11. Id.

12. S. Rep. No. 541, 99th Cong., 2nd Sess., 49 (1986).

13. 18 U.S.C.A. sec. 3126(3) (West Supp. 1988).

14. Id.

15. S. Rep. No. 541, 99th Cong., 2nd Sess., 49 (1986).

16. 18 U.S.C.A. sec. 3126(4) (West Supp. 1988).

17. S. Rep. No. 541, 99th Cong., 2nd Sess., 49 (1986).

18. 18 U.S.C.A. sec. 1821(b)(1) (West Supp. 1988).

19. Id.

20. *U.S. v. N.Y. Telephone Co.*, 434 U.S. 159, 174, 175 (1977).

21. 18 U.S.C.A. sec. 3121(b)(2) (West Supp. 1988).

22. 18 U.S.C.A. sec. 3121(b)(2) (West Supp. 1988).

23. Fishman, Pen Registers and Privacy: Risks, Expectations and the Nullification of Congressional Intent, 29 Cath. L Rev. 557, 558 (1980).

24. Claerout, The Pen Register, 20 Drake L. Rev. 108, 109, 110 (1970).

25. 18 U.S.C.A. sec. 3121(b)(3) (West Supp. 1988).

26. 18 U.S.C.A. sec 3121(c) (West Supp. 1988).

27. 18 U.S.C.A. sec 3122(a)(1) (West Supp. 1988).

28. 18 U.S.C.A. sec 3122(a)(2) (West Supp. 1988).

29. 18 U.S.C.A. sec 3122(a)(1)(2) (West Supp. 1988).

30. 18 U.S.C.A. sec 3122(b)(1) (West Supp. 1988).

31. 18 U.S.C.A. sec 3122(b)(2) (West Supp. 1988).

32. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All U.S. Attorneys and Strike Force Chiefs, December 15, 1986, 30.

33. S. Rep. No. 541, 99th Cong., 2nd Sess., 46 (1986).

34. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 76 (1986).

35. 18 U.S.C.A. sec. 3124(d)(e) (West Supp. 1988).

36. 18 U.S.C.A. sec. 3123(a) (West Supp. 1988).

37. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All States Attorneys and Strike Force Chiefs, December 15, 1986, 30.

38. S. Rep. No. 54, 99th Cong., 2nd Sess., 47 (1986).

39. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 77 (1986).

40. S. Rep. No. 541, 99th Cong., 2nd Sess., 47 (1986).

41. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All States Attorneys and Strike Force Chiefs, December 15, 1986, 31.

42. Id.

43. 18 U.S.C.A. sec. 3123(b)(1)(A) (West Supp. 1988).

44. 18 U.S.C.A. sec. 3123(b)(1)(B) (West Supp. 1988).

45. 18 U.S.C.A. sec. 3123(b)(1)(C) (West Supp. 1988).

46. Id.

47. 18 U.S.C.A. sec. 3123(b)(2) (West Supp. 1988).

48. 18 U.S.C.A. sec. 3123(b)(2) (West Supp. 1988).

49. S. Rep. No. 541, 99th Cong., 2nd Sess., 47 (1986).

50. 18 U.S.C.A. sec. 3123(d)(2) (West Supp. 1988).

51. 18 U.S.C.A. sec. 3123(d)(2) (West Supp. 1988).

52. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 77 (1986).

53. 18 U.S.C.A. sec. 3123(d)(1) (West Supp. 1988).

54. 18 U.S.C.A. sec. 3123(c)(1) (West Supp. 1988).

55. 18 U.S.C.A. Sec. 3123(c)(2) (West Supp. 1988).

56. William F. Weld, Assistant Attorney General, Criminal Division, Memorandum to All States Attorneys and Strike Force Chiefs, December 15, 1986, 31.

57. 18 U.S.C.A. sec. 3124(a) (West Supp. 1988).

58. S. Rep. No. 541, 99th Cong., 2nd Sess., 48 (1986).

59. 18 U.S.C.A. sec. 3124(b) (West Supp. 1988).

60. William Weld at 32.

61. 18 U.S.C.A. sec. 3124(b) (West Supp. 1988).

62. 18 U.S.C.A. sec. 3124(b) (West Supp. 1988).

63. William Weld at 32.

64. 18 U.S.C.A. sec. 3124(c) (West Supp. 1988).

65. H.R. Rep. No. 647, 99th Cong., 2nd Sess., 52 (1986).

66. S. Rep. No. 541, 99th Cong., 2nd Sess., 43 (1986).

67. 18 U.S.C.A. sec. 3124(d) (West Supp. 1988).

68. 18 U.S.C.A. sec. 3124(e) (West Supp. 1988).

69. 18 U.S.C.A. sec. 3125(a)(1) (West Supp. 1988).

70. 18 U.S.C.A. sec. 3125(a)(1) (West Supp. 1988).

71. 18 U.S.C.A. sec. 3125(a)(2) (West Supp. 1988).

72. 18 U.S.C.A. sec. 3125(b) (West Supp. 1988).

73. 18 U.S.C.A. sec. 3125(a) (West Supp. 1988).

74. 18 U.S.C.A. sec. 3125(c) (West Supp. 1988).

75. 18 U.S.C.A. sec. 3125(d) (West Supp. 1988).

The Electronic Communications Privacy Act of 1986

PUBLIC LAW 99-508—OCT. 21, 1986

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

Public Law 99-508
99th Congress

An Act

Oct. 21, 1986
[H.R. 4952]

To amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes.

Electronic Communications Privacy Act of 1986.
18 USC 2510 note.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Communications Privacy Act of 1986".

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

SEC. 101. FEDERAL PENALTIES FOR THE INTERCEPTION OF COMMUNICATIONS.

(a) DEFINITIONS.—(1) Section 2510(1) of title 18, United States Code, is amended—

(A) by striking out "any communication" and inserting "any aural transfer" in lieu thereof;

(B) by inserting "(including the use of such connection in a switching station)" after "reception".

(C) by striking out "as a common carrier" and

(D) by inserting before the semicolon at the end the following: "or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit".

(2) Section 2510(2) of title 18, United States Code, is amended by inserting before the semicolon at the end the following: ", but such term does not include any electronic communication".

(3) Section 2510(4) of title 18, United States Code, is amended—

(A) by inserting "or other" after "aural"; and

(B) by inserting ", electronic," after "wire".

(4) Section 2510(5) of title 18, United States Code, is amended in clause (a)(i) by inserting before the semicolon the following: "or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business".

(5) Section 2510(8) of title 18, United States Code, is amended by striking out "identity of the parties to such communication or the existence,".

(6) Section 2510 of title 18, United States Code, is amended—

(A) by striking out "and" at the end of paragraph (10);

(B) by striking out the period at the end of paragraph (11) and inserting a semicolon in lieu thereof; and

(C) by adding at the end the following:

"(12) 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any

nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

"(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

"(B) any wire or oral communication;

"(C) any communication made through a tone-only paging device; or

"(D) any communication from a tracking device (as defined in section 3117 of this title); 18 USC 3117.

"(13) 'user' means any person or entity who—

"(A) uses an electronic communication service; and

"(B) is duly authorized by the provider of such service to engage in such use;

"(14) 'electronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

"(15) 'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications;

"(16) 'readily accessible to the general public' means, with respect to a radio communication, that such communication is not—

"(A) scrambled or encrypted;

"(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

"(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

"(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

"(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

"(17) 'electronic storage' means—

"(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

"(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

"(18) 'aural transfer' means a transfer containing the human voice at any point between and including the point of origin and the point of reception.".

(b) EXCEPTIONS WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—

(1) Section 2511(2)(a)(ii) of title 18, United States Code, is amended—

(A) by striking out "violation of this subparagraph by a communication common carrier or an officer, employee, or agent thereof" and inserting in lieu thereof "such disclosure";

(B) by striking out "the carrier" and inserting in lieu thereof "such person"; and

(C) by striking out "an order or certification under this subparagraph" and inserting in lieu thereof "a court order or certification under this chapter".

(2) Section 2511(2)(d) of title 18, United States Code, is amended by striking out "or for the purpose of committing any other injurious act".

(3) Section 2511(2)(f) of title 18, United States Code, is amended—

(A) by inserting "or chapter 121" after "this chapter"; and

(B) by striking out "by" the second place it appears and inserting in lieu thereof ", or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing".

(4) Section 2511(2) of title 18, United States Code, is amended by adding at the end the following:

"(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

Post, p. 1860.

"(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

"(ii) to intercept any radio communication which is transmitted—

"(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

"(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

"(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

"(IV) by any marine or aeronautical communications system;

"(iii) to engage in any conduct which—

"(I) is prohibited by section 633 of the Communications Act of 1934; or

47 USC 553.

"(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

47 USC 605.

"(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

"(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

"(h) It shall not be unlawful under this chapter—

"(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

Post, p. 1868.

"(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.".

(c) TECHNICAL AND CONFORMING AMENDMENTS.—(1) Chapter 119 of title 18, United States Code, is amended—

18 USC 2510 *et seq.*

(A) in each of sections 2510(5), 2510(8), 2510(9)(b), 2510(11), and 2511 through 2519 (except sections 2515, 2516(1) and 2518(10)), by striking out "wire or oral" each place it appears (including in any section heading) and inserting "wire, oral, or electronic" in lieu thereof; and

(B) in section 2511(2)(b), by inserting "or electronic" after "wire".

(2) The heading of chapter 119 of title 18, United States Code, is amended by inserting "and electronic communications" after "wire".

(3) The item relating to chapter 119 in the table of chapters at the beginning of part I of title 18 of the United States Code is amended by inserting "and electronic communications" after "Wire".

(4) Section 2510(5)(a) of title 18, United States Code, is amended by striking out "communications common carrier" and inserting "provider of wire or electronic communication service" in lieu thereof.

(5) Section 2511(2)(a)(i) of title 18, United States Code, is amended—

(A) by striking out "any communication common carrier" and inserting "a provider of wire or electronic communication service" in lieu thereof;

(B) by striking out "of the carrier of such communication" and inserting "of the provider of that service" in lieu thereof; and

(C) by striking out ": *Provided,* That said communication common carriers" and inserting ", except that a provider of wire communication service to the public" in lieu thereof.

(6) Section 2511(2)(a)(ii) of title 18, United States Code, is amended—

(A) by striking out "communication common carriers" and inserting "providers of wire or electronic communication service" in lieu thereof;

(B) by striking out "communication common carrier" each place it appears and inserting "provider of wire or electronic communication service" in lieu thereof; and

(C) by striking out "if the common carrier" and inserting "if such provider" in lieu thereof.

(7) Section 2512(2)(a) of title 18, United States Code, is amended—

(A) by striking out "a communications common carrier" the first place it appears and inserting "a provider of wire or electronic communication service" in lieu thereof; and

(B) by striking out "a communications common carrier" the second place it appears and inserting "such a provider" in lieu thereof; and

(C) by striking out "communications common carrier's business" and inserting "business of providing that wire or electronic communication service" in lieu thereof.

(8) Section 2518(4) of title 18, United States Code, is amended—

(A) by striking out "communication common carrier" in both places it appears and inserting "provider of wire or electronic communication service" in lieu thereof; and

(B) by striking out "carrier" and inserting in lieu thereof "service provider".

(d) PENALTIES MODIFICATION.—(1) Section 2511(1) of title 18, United States Code, is amended by striking out "shall be" and all that follows through "or both" and inserting in lieu thereof "shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5)".

(2) Section 2511 of title 18, United States Code, is amended by adding after the material added by section 102 the following:

"(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

"(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled or encrypted, then—

"(i) if the communication is not the radio portion of a cellular telephone communication, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both; and

"(ii) if the communication is the radio portion of a cellular telephone communication, a public land mobile radio service communication or a paging service communication, the offender shall be fined not more than $500.

"(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted—

"(i) to a broadcasting station for purposes of retransmission to the general public; or

"(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

"(5)(a)(i) If the communication is—

"(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

"(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for

-A-4-

a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

"(ii) In an action under this subsection—

"(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and *Infra.*

"(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

"(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.".

(e) EXCLUSIVITY OF REMEDIES WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—Section 2518(10) of title 18, United States Code, is amended by adding at the end the following:

"(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.".

(f) STATE OF MIND.—Paragraphs (a), (b), (c), and (d) of subsection (1) of section 2511 of title 18, United States Code, are amended by striking out "willfully" and inserting in lieu thereof "intentionally".

(2) Subsection (1) of section 2512 of title 18, United States Code, is amended in the matter before paragraph (a) by striking out "willfully" and inserting in lieu thereof "intentionally".

SEC. 102. REQUIREMENTS FOR CERTAIN DISCLOSURES.

Section 2511 of title 18, United States Code, is amended by adding at the end the following:

"(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

"(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

"(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

"(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

"(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

"(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.".

SEC. 103. RECOVERY OF CIVIL DAMAGES.

Section 2520 of title 18, United States Code, is amended to read as follows:

"§ 2520. Recovery of civil damages authorized

"(a) IN GENERAL.—Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) RELIEF.—In an action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c) and punitive damages in appropriate cases; and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) COMPUTATION OF DAMAGES.—(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

"(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

"(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.

"(2) In any other action under this section, the court may assess as damages whichever is the greater of—

"(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

"(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

"(d) DEFENSE.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

"(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.".

-4-5-

SEC. 104. CERTAIN APPROVALS BY JUSTICE DEPARTMENT OFFICIALS.

Section 2516(1) of title 18 of the United States Code is amended by striking out "or any Assistant Attorney General" and inserting in lieu thereof "any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division".

SEC. 105. ADDITION OF OFFENSES TO CRIMES FOR WHICH INTERCEPTION IS AUTHORIZED.

(a) WIRE AND ORAL INTERCEPTIONS.—Section 2516(1) of title 18 of the United States Code is amended—

(1) in paragraph (c)—

(A) by inserting "section 751 (relating to escape)," after "wagering information),";

(B) by striking out "2314" and inserting "2312, 2313, 2314," in lieu thereof;

(C) by inserting "the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities)," after "stolen property),"; Motor vehicles. Aircraft and air carriers.

(D) by inserting "section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity)," after "1952 (interstate and foreign travel or transportation in aid of racketeering enterprises),";

(E) by inserting ", section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud)," after "section 1963 (violations with respect to racketeer influenced and corrupt organizations)"; and Energy. Mail. Fraud.

(F) by— Hazardous materials. Motor vehicles.

(i) striking out "or" before "section 351" and inserting in lieu thereof a comma; and

(ii) inserting before the semicolon at the end thereof the following: ", section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), or section 1992 (relating to wrecking trains)";

(2) by striking out "or" at the end of paragraph (g);

(3) by inserting after paragraph (g) the following:

"(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

"(i) any violation of section 1679a(c)(2) (relating to destruction of a natural gas pipeline) or subsection (i) or (n) of section 1472 (relating to aircraft piracy) of title 49, of the United States Code; Natural gas. Aircraft and air carriers.

"(j) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act); or"; 22 USC 2751 note.

"(k) the location of any fugitive from justice from an offense described in this section;

(4) by redesignating paragraph (h) as paragraph (l); and

(5) in paragraph (a) by—

Hazardous materials.

(A) inserting after "Atomic Energy Act of 1954)," the following: "section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel),";

(B) striking out "or" after "(relating to treason),"; and

18 USC 1361 et seq.
18 USC 2271 et seq.
Vessels.
18 USC 1651 et seq.

(C) inserting before the semicolon at the end thereof the following: "chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy)".

(b) INTERCEPTION OF ELECTRONIC COMMUNICATIONS.—Section 2516 of title 18 of the United States Code is amended by adding at the end the following:

18 USC app.

"(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.".

SEC. 106. APPLICATIONS, ORDERS, AND IMPLEMENTATION OF ORDERS.

(a) PLACE OF AUTHORIZED INTERCEPTION.—Section 2518(3) of title 18 of the United States Code is amended by inserting "(and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction)" after "within the territorial jurisdiction of the court in which the judge is sitting".

(b) REIMBURSEMENT FOR ASSISTANCE.—Section 2518(4) of title 18 of the United States Code is amended by striking out "at the prevailing rates" and inserting in lieu thereof "for reasonable expenses incurred in providing such facilities or assistance".

(c) COMMENCEMENT OF THIRTY-DAY PERIOD AND POSTPONEMENT OF MINIMIZATION.—Section 2518(5) of title 18 of the United States Code is amended—

(1) by inserting after the first sentence the following: "Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered."; and

(2) by adding at the end the following: "In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.".

(d) ALTERNATIVE TO DESIGNATING SPECIFIC FACILITIES FROM WHICH COMMUNICATIONS ARE TO BE INTERCEPTED.—(1) Section 2518(1)(b)(ii) of title 18 of the United States Code is amended by inserting "except as provided in subsection (11)," before "a particular description".

(2) Section 2518(3)(d) of title 18 of the United States Code is amended by inserting "except as provided in subsection (11)," before "there is".

(3) Section 2518 of title 18 of the United States Code is amended by adding at the end the following:

"(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

"(a) in the case of an application with respect to the interception of an oral communication—

"(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

"(iii) the judge finds that such specification is not practical; and

"(b) in the case of an application with respect to a wire or electronic communication—

"(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

"(iii) the judge finds that such purpose has been adequately shown.

"(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.".

(4) Section 2519(1)(b) of title 18, United States Code, is amended by inserting "(including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title)" after "applied for".

18 USC 2510 note.

SEC. 107. INTELLIGENCE ACTIVITIES.

(a) IN GENERAL.—Nothing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity.

(b) CERTAIN ACTIVITIES UNDER PROCEDURES APPROVED BY THE ATTORNEY GENERAL.—Nothing in chapter 119 or chapter 121 of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to—

18 USC 2510 *et seq.*; *post*, p. 1860.

(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;

(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978; or

50 USC 1801 note.

(3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978.

SEC. 108. MOBILE TRACKING DEVICES.

(a) IN GENERAL.—Chapter 205 of title 18, United States Code, is amended by adding at the end the following:

18 USC 3117.

"§ 3117. Mobile tracking devices

"(a) IN GENERAL.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

"(b) DEFINITION.—As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object.".

(b) CLERICAL AMENDMENT.—The table of contents at the beginning of chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"3117. Mobile tracking devices.".

SEC. 109. WARNING SUBJECT OF SURVEILLANCE.

Section 2232 of title 18, United States Code, is amended—

(1) by inserting "(a) PHYSICAL INTERFERENCE WITH SEARCH.—" before "Whoever" the first place it appears;

(2) by inserting "(b) NOTICE OF SEARCH.—" before "Whoever" the second place it appears; and

(3) by adding at the end the following:

Law enforcement and crime. 18 USC 2510 *et seq.*; *post*, p. 1859.

"(c) NOTICE OF CERTAIN ELECTRONIC SURVEILLANCE.—Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both.

"Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years, or both.".

-A-7-

SEC. 110. INJUNCTIVE REMEDY.

(a) IN GENERAL.—Chapter 119 of title 18, United States Code, is amended by adding at the end the following:

"§ 2521. Injunction against illegal interception 18 USC 2521.

"Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.". 28 USC app. 18 USC app.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 119 of title 18, United States Code, is amended by adding at the end thereof the following:

"2521. Injunction against illegal interception.".

SEC. 111. EFFECTIVE DATE. 18 USC 2510 note.

(a) IN GENERAL.—Except as provided in subsection (b) or (c), this title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any interception pursuant to section 2516(2) of title 18 of the United States Code which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such interception occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of State law conforming the applicable State statute with chapter 119 of title 18, United States Code, as so amended; or 18 USC 2510 *et seq.*

(2) the date two years after the date of the enactment of this Act.

(c) EFFECTIVE DATE FOR CERTAIN APPROVALS BY JUSTICE DEPARTMENT OFFICIALS.—Section 104 of this Act shall take effect on the date of enactment of this Act.

TITLE II—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

SEC. 201. TITLE 18 AMENDMENT.

Title 18, United States Code, is amended by inserting after chapter 119 the following:

"CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

USC 2701.

"§ 2701. Unlawful access to stored communications

"(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—

"(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

"(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

"(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

"(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—

"(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

"(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.

"(c) EXCEPTIONS.—Subsection (a) of this section does not apply with respect to conduct authorized—

"(1) by the person or entity providing a wire or electronic communications service;

"(2) by a user of that service with respect to a communication of or intended for that user; or

"(3) in section 2703, 2704 or 2518 of this title.

18 USC 2702.

"§ 2702. Disclosure of contents

"(a) PROHIBITIONS.—Except as provided in subsection (b)—

-8-

"(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

"(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

"(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

"(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

"(b) EXCEPTIONS.—A person or entity may divulge the contents of a communication—

"(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

"(2) as otherwise authorized in section 2516, 2511(2)(a), or 2703 of this title; 18 USC 2516, 2511; *infra*.

"(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

"(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

"(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

"(6) to a law enforcement agency, if such contents—

"(A) were inadvertently obtained by the service provider; and

"(B) appear to pertain to the commission of a crime.

"§ 2703. Requirements for governmental access

State and local governments. 18 USC 2703.

"(a) CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section. 18 USC app.

"(b) CONTENTS OF ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

"(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the

18 USC app.

Federal Rules of Criminal Procedure or equivalent State warrant; or

"(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

"(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena; or

"(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

Post, p. 1864.

"(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service—

"(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

"(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

"(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1)(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

"(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity—

"(i) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury subpoena;

"(ii) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant;

"(iii) obtains a court order for such disclosure under subsection (d) of this section; or

"(iv) has the consent of the subscriber or customer to such disclosure.

"(2) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

Records.

"(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) of this section shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if

the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

"(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under this chapter.

"§ 2704. Backup preservation

18 USC 2704.

"(a) BACKUP PRESERVATION.—(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

"(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

"(3) The service provider shall not destroy such backup copy until the later of—

"(A) the delivery of the information; or

"(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

"(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider—

"(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

"(B) has not initiated proceedings to challenge the request of the governmental entity.

"(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

"(b) CUSTOMER CHALLENGES.—(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement—

"(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

"(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

"(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term 'delivery' has the meaning

28 USC app. given that term in the Federal Rules of Civil Procedure.

"(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

"(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

"(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

-A-10-

18 USC 2705.

"§ 2705. Delayed notice

"(a) Delay of Notification.—(1) A governmental entity acting under section 2703(b) of this title may—

"(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

State and local governments.

"(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the

subpoena may have an adverse result described in paragraph (2) of this subsection.

"(2) An adverse result for the purposes of paragraph (1) of this subsection is—

"(A) endangering the life or physical safety of an individual;

"(B) flight from prosecution;

"(C) destruction of or tampering with evidence;

"(D) intimidation of potential witnesses; or

"(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

"(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

"(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that—

"(A) states with reasonable specificity the nature of the law enforcement inquiry; and

"(B) informs such customer or subscriber—

"(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

"(ii) that notification of such customer or subscriber was delayed;

"(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

"(iv) which provision of this chapter allowed such delay.

"(6) As used in this subsection, the term 'supervisory official' means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

"(b) Preclusion of Notice to Subject of Governmental Access.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

"(1) endangering the life or physical safety of an individual;

"(2) flight from prosecution;

"(3) destruction of or tampering with evidence;

"(4) intimidation of potential witnesses; or

"(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 USC 2706.

"§ 2706. Cost reimbursement

"(a) PAYMENT.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

"(b) AMOUNT.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

"(c) The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

"§ 2707. Civil action

"(a) CAUSE OF ACTION.—Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) RELIEF.—In a civil action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c); and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) DAMAGES.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

"(d) DEFENSE.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

"(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

"§ 2708. Exclusivity of remedies 18 USC 2708.

"The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

"§ 2709. Counterintelligence access to telephone toll and transactional records 18 USC 2709.

"(a) DUTY TO PROVIDE.—A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

"(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the wire or electronic communication service provider to which the request is made that—

"(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

"(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

"(c) PROHIBITION OF CERTAIN DISCLOSURE.—No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

"(d) DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

"(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

18 USC 2710.

"§ 2710. Definitions for chapter

"As used in this chapter—

"(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

"(2) the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.".

(b) CLERICAL AMENDMENT.—The table of chapters at the beginning of part I of title 18, United States Code, is amended by adding at the end the following:

"121. Stored Wire and Electronic Communications and Transactional Records Access .... 2701".

18 USC 2701 note.

SEC. 202. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect ninety days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

TITLE III—PEN REGISTERS AND TRAP AND TRACE DEVICES

SEC. 301. TITLE 18 AMENDMENT.

(a) IN GENERAL.—Title 18 of the United States Code is amended by inserting after chapter 205 the following new chapter:

"CHAPTER 206—PEN REGISTERS AND TRAP AND TRACE DEVICES

"Sec.
"3121. General prohibition on pen register and trap and trace device use; exception.
"3122. Application for an order for a pen register or a trap and trace device.
"3123. Issuance of an order for a pen register or a trap or trace device.
"3124. Assistance in installation and use of a pen register or a trap and trace device.
"3125. Reports concerning pen registers and trap and trace devices.
"3126. Definitions for chapter.

18 USC 3121.

"§ 3121. General prohibition on pen register and trap and trace device use; exception

"(a) IN GENERAL.—Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(b) EXCEPTION.—The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service—

"(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

"(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained.

"(c) PENALTY.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

"§ 3122. Application for an order for a pen register or a trap and trace device 18 USC 3122.

"(a) APPLICATION.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

"(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State. State and local governments.

"(b) CONTENTS OF APPLICATION.—An application under subsection (a) of this section shall include—

"(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

"(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

"§ 3123. Issuance of an order for a pen register or a trap and trace device

"(a) IN GENERAL.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

"(b) CONTENTS OF ORDER.—An order issued under this section—

"(1) shall specify—

"(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached;

"(B) the identity, if known, of the person who is the subject of the criminal investigation;

"(C) the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and

"(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

"(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

"(c) TIME PERIOD AND EXTENSIONS.—(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.

"(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

"(d) NONDISCLOSURE OF EXISTENCE OF PEN REGISTER OR A TRAP AND TRACE DEVICE.—An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that—

"(1) the order be sealed until otherwise ordered by the court; and

"(2) the person owning or leasing the line to which the pen register or a trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

18 USC 3124.

"§ 3124. Assistance in installation and use of a pen register or a trap and trace device

"(a) PEN REGISTERS.—Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

"(b) TRAP AND TRACE DEVICE.—Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the

device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the officer of a law enforcement agency, designated in the court, at reasonable intervals during regular business hours for the duration of the order.

"(c) COMPENSATION.—A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

"(d) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order under this chapter.

"(e) DEFENSE.—A good faith reliance on a court order, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

"§ 3125. Reports concerning pen registers and trap and trace devices 18 USC 3125.

"The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice.

"§ 3126. Definitions for chapter

"As used in this chapter—

"(1) the terms 'wire communication', 'electronic communication', and 'electronic communication service' have the meanings set forth for such terms in section 2510 of this title;

"(2) the term 'court of competent jurisdiction' means—

"(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or

"(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

"(3) the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

"(4) the term 'trap and trace device' means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted;

"(5) the term 'attorney for the Government' has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

"(6) the term 'State' means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.".

(b) CLERICAL AMENDMENT.—The table of chapters for part II of title 18 of the United States Code is amended by inserting after the item relating to chapter 205 the following new item:

18 USC 3121 note.

SEC. 302. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title shall take effect ninety days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any pen register or trap and trace device order or installation which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such order or installation occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of changes in State law required in order to make orders or installations under Federal law as amended by this title; or

(2) the date two years after the date of the enactment of this Act.

SEC. 303. INTERFERENCE WITH THE OPERATION OF A SATELLITE.

(a) OFFENSE.—Chapter 65 of title 18, United States Code, is amended by inserting at the end the following:

18 USC 1367.

"§ 1367. Interference with the operation of a satellite

"(a) Whoever, without the authority of the satellite operator, intentionally or maliciously interferes with the authorized operation of a communications or weather satellite or obstructs or hinders any satellite transmission shall be fined in accordance with this title or imprisoned not more than ten years or both.

"(b) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency or of an intelligence agency of the United States."

(b) CONFORMING AMENDMENT.—The table of sections for chapter 65 of title 18, United States Code, is amended by adding at the end the following new item:

Approved October 21, 1986.

LEGISLATIVE HISTORY—H.R. 4952 (S. 2575):

HOUSE REPORTS: No. 99-647 (Comm. on the Judiciary).
CONGRESSIONAL RECORD, Vol. 132 (1986):
June 23, considered and passed House.
Oct. 1, considered and passed Senate, amended.
Oct. 2, House concurred in Senate amendments.

O

House of Representatives
Report Number 99-647

99TH CONGRESS *2d Session*	HOUSE OF REPRESENTATIVES	REPORT 99-647

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

JUNE 19, 1986.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. KASTENMEIER, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany H.R. 4952]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 4952) to amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Communications Privacy Act of 1986".

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

SEC. 101. FEDERAL PENALTIES FOR THE INTERCEPTION OF COMMUNICATIONS.

(a) DEFINITIONS.—(1) Section 2510(1) of title 18, United States Code, is amended—

(A) by striking out "any communication" and inserting "any aural transfer" in lieu thereof;

(B) by inserting "(including the use of such connection in a switching station)" after "reception".

(C) by striking out "as a common carrier" and

(D) by inserting before the semicolon at the end the following: "or communications affecting interstate or foreign commerce, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit".

(2) Section 2510(2) of title 18, United States Code, is amended by inserting before the semicolon at the end the following: ", but such term does not include any electronic communication".

(3) Section 2510(4) of title 18, United States Code, is amended—

(A) by inserting "or other" after "aural"; and

61-068 O

(B) by inserting ", electronic," after "wire".

(4) Section 2510(8) of title 18, United States Code, is amended by striking out "identity of the parties to such communication or the existence,".

(5) Section 2510 of title 18, United States Code, is amended—

(A) by striking out "and" at the end of paragraph (10);

(B) by striking out the period at the end of paragraph (11) and inserting a semicolon in lieu thereof; and

(C) by adding at the end the following:

"(12) 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

"(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

"(B) any wire or oral communication;

"(C) any communication made through a tone-only paging device; or

"(D) any communication from a tracking device (as defined in section 3117 of this title);

"(13) 'user' means any person or entity who—

"(A) uses an electronic communication service; and

"(B) is duly authorized by the provider of such service to engage in such use;

"(14) 'electronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

"(15) 'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications;

"(16) 'readily accessible to the general public' means, with respect to a radio communication, that such communication is not—

"(A) scrambled or encrypted;

"(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

"(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

"(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

"(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

"(17) 'electronic storage' means—

"(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

"(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

"(18) 'aural transfer' means a transfer containing the human voice at any point between and including the point of origin and the point of reception.".

(b) EXCEPTIONS WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—

(1) Section 2511(2)(d) of title 18, United States Code, is amended by striking out "or for the purpose of committing any other injurious act".

(2) Section 2511(2)(f) of title 18, United States Code is amended—

(A) by inserting "or chapter 121" after "this chapter", and

(B) by striking out "by" the second place it appears and inserting in lieu thereof ", or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing".

(3) Section 2511(2) of title 18, United States Code, is amended by adding at the end the following:

"(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

"(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

"(ii) to intercept any radio communication which is transmitted—

"(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

"(II) by any governmental, law enforcement, civil defense, or public safety communications system, including police and fire, readily accessible to the general public;

"(III) by a station operating on a frequency assigned to the amateur, citizens band, or general mobile radio services; or

"(IV) by any marine or aeronautical communications system;

"(iii) to engage in any conduct which—

"(I) is prohibited by section 633 of the Communications Act of 1934; or

"(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

"(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of such interference; or

"(v) for other users of the same frequency to intercept any radio communication made through a common carrier system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

"(h) It shall not be unlawful under this chapter—

"(i) to use a pen register (as that term is defined for the purposes of chapter 206 (relating to pen registers) of this title);

"(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service; or

"(iii) to use a device that captures the incoming electronic or other impulses which identify the numbers of an instrument from which a wire communication was transmitted".

(c) TECHNICAL AND CONFORMING AMENDMENTS.—(1) Chapter 119 of title 18, United States Code, is amended—

(A) in each of sections 2510(5), 2510(8), 2510(9)(b), 2510(11), and 2511 through 2519 (except sections 2516(1) and 2518(10)), by striking out "wire or oral" each place it appears (including in any section heading) and inserting "wire, oral, or electronic" in lieu thereof; and

(B) in section 2511(2)(b), by inserting "or electronic" after "wire".

(2) The heading of chapter 119 of title 18, United States Code, is amended by inserting "and electronic communications" after "wire".

(3) The item relating to chapter 119 in the table of chapters at the beginning of part I of title 18 of the United States Code is amended by inserting "and electronic communications" after "Wire".

(4) Section 2510(5)(a) of title 18, United States Code, is amended by striking out "communications common carrier" and inserting "provider of wire or electronic communication service" in lieu thereof.

(5) Section 2511(2)(a)(i) of title 18, United States Code, is amended—

(A) by striking out "any communication common carrier" and inserting "a provider of wire or electronic communication service" in lieu thereof;

(B) by striking out "of the carrier of such communication" and inserting "of the provider of that service" in lieu thereof; and

(C) by striking out ": Provided, That said communication common carriers" and inserting ", except that a provider of wire communication service to the public" in lieu thereof.

(6) Section 2511(2)(a)(ii) of title 18, United States Code, is amended—

(A) by striking out "communication common carriers" and inserting "providers of wire or electronic communication service" in lieu thereof;

(B) by striking out "communication common carrier" each place it appears and inserting "provider of wire or electronic communication service" in lieu thereof; and

(C) by striking out "if the common carrier" and inserting "if such provider" in lieu thereof.

(7) Section 2518(4) of title 18, United States Code, is amended—

(A) by striking out "a communications common carrier" the first place it appears and inserting "a provider of wire or electronic communication service" in lieu thereof; and

(B) by striking out "a communications common carrier" the second place it appears and inserting "such a provider" in lieu thereof; and

(C) by striking out "communications common carrier's business" and inserting "business of providing that wire or electronic communication service" in lieu thereof.

(8) Section 2518(4) of title 18, United States Code, is amended by striking out "communication common carrier" and inserting "provider of electronic communication service" in lieu thereof.

(d) PENALTIES MODIFICATION.—(1) Section 2511(1) of title 18, United States Code, is amended by striking out "shall be" and all that follows through "or both" and inserting in lieu thereof "shall be punished as provided in subsection (4)".

(2) Section 2511 of title 18, United States Code, is amended by adding after the material added by section 102 the following:

"(4)(a) Except as provided in paragraph (b) of this subsection, whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

"(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication, then—

"(i) if the communication is not the radio portion of a cellular telephone communication, the offender shall be fined under this title or imprisoned not more than one year, or both; and

"(ii) if the communication is the radio portion of a cellular telephone communication, the offender shall be fined not more than $500 or imprisoned not more than six months, or both.

"(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of retransmission to the general public is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.".

(e) EXCLUSIVITY OF REMEDIES WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—Section 2518(10) of title 18, United States Code, is amended by adding at the end the following:

"(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.".

SEC. 102. REQUIREMENTS FOR CERTAIN DISCLOSURES.

Section 2511 of title 18, United States Code, is amended by adding at the end the following:

"(3)(a) Except as provided in subparagraph (b) of this paragraph, a person or entity providing an electronic communication service to the public shall not willfully divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

"(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

"(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

"(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

"(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

"(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.".

SEC. 103. RECOVERY OF CIVIL DAMAGES.

Section 2520 of title 18, United States Code, is amended to read as follows:

"§ 2520. Recovery of civil damages authorized

"(a) IN GENERAL.—Any person whose wire, oral, or electronic communication is intercepted, disclosed, or willfully used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) RELIEF.—In an action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c) and punitive damages in appropriate cases; and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) COMPUTATION OF DAMAGES.—The court may assess as damages in an action under this section whichever is the greater of—

"(1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

"(2) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

"(d) DEFENSE.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other provision of law.

"(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.".

SEC. 104. CERTAIN APPROVALS BY JUSTICE DEPARTMENT OFFICIALS.

Section 2516(1) of title 18 of the United States Code is amended by striking out "or any Assistant Attorney General" and inserting in lieu thereof "any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division".

SEC. 105. ADDITION OF OFFENSES TO CRIMES FOR WHICH INTERCEPTION IS AUTHORIZED.

(a) WIRE AND ORAL INTERCEPTIONS.—Section 2516(1) of title 18 of the United States Code is amended—

(1) in paragraph (c)—

(A) by inserting "section 751 (relating to escape)," after "wagering information),";

(B) by striking out "2314" and inserting "2312, 2313, 2314," in lieu thereof;

(C) by inserting "the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities)," after "stolen property),";

(D) by inserting "section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity)," after "1952 (interstate and foreign travel or transportation in aid of racketeering enterprises),"; and

(E) by inserting ", section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud)," after "section 1963 (violations with respect to racketeer influenced and corrupt organizations)";

(2) by striking out "or" at the end of paragraph (g);

(3) by inserting after paragraph (g) the following:

"(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

"(i) the location of any fugitive from justice from an offense described in this section; or"; and

(4) by redesignating paragraph (h) as paragraph (j).

(b) INTERCEPTION OF ELECTRONIC COMMUNICATIONS.—Section 2516 of title 18 of the United States Code is amended by adding at the end the following:

"(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.".

SEC. 106. APPLICATIONS, ORDERS, AND IMPLEMENTATION OF ORDERS.

(a) PLACE OF AUTHORIZED INTERCEPTION.—Section 2518(3) of title 18 of the United States Code is amended by inserting "(and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction)" after "within the territorial jurisdiction of the court in which the judge is sitting".

(b) REIMBURSEMENT FOR ASSISTANCE.—Section 2518(4) of title 18 of the United States Code is amended by striking out "at the prevailing rates" and inserting in lieu thereof "for reasonable expenses incurred in providing such facilities or assistance".

(c) COMMENCEMENT OF 30-DAY PERIOD AND POSTPONEMENT OF MINIMIZATION.—Section 2518(5) of title 18 of the United States Code is amended—

(1) by inserting after the first sentence the following: "Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered."; and

(2) by adding at the end the following: "In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception."

(d) ALTERNATIVE TO DESIGNATING SPECIFIC FACILITIES FROM WHICH COMMUNICATIONS ARE TO BE INTERCEPTED.—(1) Section 2518(1)(b)(ii) of title of the United States Code is amended by inserting "except as provided in subsection (11)," before "a particular description".

(2) Section 2518(3)(d) of title 18 of the United States Code is amended by inserting "except as provided in subsection (11)," before "there is".

(3) Section 2518 of title 18 of the United States Code is amended by adding at the end the following:

"(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

"(i) in the case of an application with respect to the interception of an oral communication—

"(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(II) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

"(III) the judge finds that such specification is not practical; and

"(ii) in the case of an application with respect to a wire or electronic communication—

"(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(II) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

"(III) the judge finds that such purpose has been adequately shown.

"(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order.".

(4) Section 2519(1)(b) of title 18, United States Code, is amended by inserting "(including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title)" after "applied for".

SEC. 107. INTELLIGENCE ACTIVITIES.

(a) IN GENERAL.—Nothing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity.

(b) CERTAIN ACTIVITIES UNDER PROCEDURES APPROVED BY THE ATTORNEY GENERAL.—Nothing in chapter 119 or chapter 121 of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to—

(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;

(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978; or

(3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978.

SEC. 108. MOBILE TRACKING DEVICES.

(a) IN GENERAL.—Chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"§ 3117. Mobile tracking devices

"(a) IN GENERAL.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

"(b) DEFINITION.—As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object.".

(b) CLERICAL AMENDMENT.—The table of contents at the beginning of chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"3117. Mobile tracking devices.".

SEC. 109. WARNING SUBJECT OF SURVEILLANCE.

Section 2232 of title 18, United States Code, is amended—

(1) by inserting "(a) PHYSICAL INTERFERENCE WITH SEARCH.—" before "Whoever" the first place it appears;

(2) by inserting "(b) NOTICE OF SEARCH.—" before "Whoever" the second place it appears; and

(3) by adding at the end the following:

"(c) NOTICE OF CERTAIN ELECTRONIC SURVEILLANCE.—Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both.

"Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years or both.".

SEC. 110. INJUNCTIVE REMEDY.

(a) IN GENERAL.—Chapter 119 of title 18, United States Code, is amended by adding at the end the following:

"§ 2521. Injunction against illegal interception

"Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 119 of title 18, United States Code, is amended by adding at the end thereof the following:

"2521. Injunction against illegal interception.".

SEC. 111. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any interception pursuant to section 2516(2) of title 18 of the United States Code which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such interception occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of State law conforming the applicable State statute with chapter 119 of title 18, United States Code, as so amended, or

(2) the date two years after the date of the enactment of this Act.

TITLE II—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

SEC. 201. TITLE 18 AMENDMENT.

Title 18, United States Code, is amended by inserting after chapter 119 the following:

"CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

"§ 2701. Unlawful access to stored communications

"(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—

"(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

"(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

"(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

"(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—

"(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph, and

"(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

"(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.

"(c) EXCEPTIONS.—Subsection (a) of this section does not apply with respect to conduct authorized—

"(1) by the person or entity providing a wire or electronic communications service;

"(2) by a user of that service with respect to a communication of or intended for that user; or

"(3) in section 2703 or 2704 of this title.

"§ 2702. Disclosure of contents

"(a) PROHIBITIONS.—Except as provided in subsection (b)—

"(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

"(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

"(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

"(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

"(b) EXCEPTIONS.—A person or entity may divulge the contents of a communication—

"(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

"(2) as otherwise authorized in section 2516, 2511(2)(a), or 2703 of this title;

"(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

"(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

"(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

"(6) to a law enforcement agency, if such contents—

"(A) were inadvertently obtained by the service provider; and

"(B) appear to pertain to the commission of a crime.

"§ 2703. Requirements for governmental access

"(a) CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a non-voice wire communication or an electronic communication, that is in electronic storage in an electronic communications system for 180 days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than 180 days by the means available under subsection (b) of this section.

"(b) CONTENTS OF ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

"(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

"(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

"(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena; or

"(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

"(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service—

"(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

"(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

"(c) Records Concerning Electronic Communication Service or Remote Computing Service.—A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) without required notice to the subscriber or customer if the governmental entity—

"(1) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury subpoena;

"(2) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

"(3) obtains a court order for such disclosure under subsection (d) of this section.

"(d) Requirements for Court Order.—A court order for disclosure under subsection (b) or (c) of this section shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State.

"§ 2704. Backup preservation

"(a) Backup Preservation.—(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

"(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

"(3) The service provider shall not destroy such backup copy until the later of—

"(A) the delivery of the information; or

"(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

"(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than 14 days after the governmental entity's notice to the subscriber or customer if such service provider—

"(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

"(B) has not initiated proceedings to challenge the request of the governmental entity.

"(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering

with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

"(b) Customer Challenges.—(1) Within 14 days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement—

"(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

"(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

"(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term 'delivery' has the meaning given that term in the Federal Rules of Civil Procedure.

"(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

"(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

"(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

"§ 2705. Delayed notice

"(a) Delay of Notification.—(1) A governmental entity acting under section 2703(b) of this title may—

"(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed 90 days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

"(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed 90 days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

"(2) An adverse result for the purposes of paragraph (1) of this subsection is—

"(A) endangering the life or physical safety of an individual;

"(B) flight from prosecution;

"(C) destruction of or tampering with evidence;

"(D) intimidation of potential witnesses; or

"(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

"(4) Extensions of the delay of notification provided in section 2703 of up to 90 days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) or (c) of this section.

"(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first class mail to, the customer or subscriber a copy of the process or request together with notice that—

"(A) states with reasonable specificity the nature of the law enforcement inquiry; and

"(B) informs such customer or subscriber—

"(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

"(ii) that notification of such customer or subscriber was delayed;

"(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

"(iv) which provision of this chapter allowed such delay.

"(6) As used in this subsection, the term 'supervisory official' means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

"(b) Preclusion of Notice to Subject of Governmental Access.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

"(1) endangering the life or physical safety of an individual;

"(2) flight from prosecution;

"(3) destruction of or tampering with evidence;

"(4) intimidation of potential witnesses; or

"(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"§ 2706. Cost reimbursement

"(a) Payment.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

"(b) Amount.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

"(c) The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

"§ 2707. Civil action

"(a) Cause of Action.—Any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct

constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) Relief.—In a civil action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c); and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) Damages.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

"(d) Defense.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

"(e) Limitation.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

"§ 2708. Exclusivity of remedies

"The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

"§ 2709. Counterintelligence access to telephone toll and transactional records

"(a) Duty to Provide.—A communications common carrier or an electronic communication service provider shall comply with a request made for telephone subscriber information and toll billing records information, or electronic communication transactional records made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

"(b) Required Certification.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the carrier or provider to which the request is made that—

"(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

"(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

"(c) Prohibition of Certain Disclosure.—No communications common carrier or service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

"(d) Dissemination by Bureau.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

"(e) Requirement That Certain Congressional Bodies Be Informed.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

"§ 2710. Definitions for chapter

"As used in this chapter—

"(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

14

"(2) the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system."

(b) Clerical Amendment.—The table of chapters at the beginning of part I of title 18, United States Code, is amended by adding at the end the following:

"121. Stored Wire and Electronic Communications and Transactional Records Access .... 2701".

SEC. 202. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

TITLE III—PEN REGISTERS

SEC. 301. TITLE 18 AMENDMENT.

(a) In General.—Title 18 of the United States Code is amended by inserting after chapter 205 the following new chapter:

"CHAPTER 206—PEN REGISTERS

"Sec.
"3121. General prohibition on pen register use; exception.
"3122. Application for an order for a pen register.
"3123. Issuance of an order for a pen register.
"3124. Assistance in installation and use of a pen register.
"3125. Reports concerning pen registers.
"3126. Definitions for chapter.

"§ 3121. General prohibition on pen register use; exception

"(a) In General.—Except as provided in this section, no person may install or use a pen register without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(b) Exception.—The prohibition of subsection (a) does not apply with respect to the use of a pen register by a provider of electronic or wire communication service—

"(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

"(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service, or with the consent of the user of that service.

"(c) Penalty.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

"§ 3122. Application for an order for a pen register

"(a) Application.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

"(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

"(b) Contents of Application.—An application under subsection (a) of this section shall include—

"(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

"(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

15

"§ 3123. Issuance of an order for a pen register

"(a) In General.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

"(b) Contents of Order.—An order issued under this section—

"(1) shall specify—

"(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register is to be attached;

"(B) the identity, if known, of the person who is the subject of the criminal investigation;

"(C) the number and, if known, physical location of the telephone line to which the pen register is to be attached; and

"(D) a statement of the offense to which the information likely to be obtained by the pen register relates; and

"(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register under section 3124 of this title.

"(c) Time Period and Extensions.—(1) An order issued under this section shall authorize the installation and use of a pen register for a period not to exceed 60 days.

"(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed 60 days.

"(d) Nondisclosure of Existence of Pen Register.—An order authorizing or approving the installation and use of a pen register shall direct that—

"(1) the order be sealed until otherwise ordered by the court; and

"(2) the person owning or leasing the line to which the pen register is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

"§ 3124. Assistance in installation and use of a pen register

"(a) In General.—Upon the request of an attorney for the government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

"(b) Compensation.—A provider of wire communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

"§ 3125. Reports concerning pen registers

"The Attorney General shall annually report to Congress on the number of pen register orders applied for by law enforcement agencies of the Department of Justice.

"§ 3126. Definitions for chapter

"As used in this chapter—

"(1) the term 'communications common carrier' has the meaning set forth for the term 'common carrier' in section 3(h) of the Communications Act of 1934 (47 U.S.C. 153(h));

"(2) the term 'wire communication' has the meaning set forth for such term in section 2510 of this title;

"(3) the term 'court of competent jurisdiction' means—

"(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or

"(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register;

16

"(4) the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted, with respect to wire communications, on the telephone line to which such device is attached, but such term does not include any device used by a provider of wire communication service for billing, or recording as an incident to billing, for communications services provided by such provider; and

"(5) the term 'attorney for the Government' has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

"(6) the term 'State' means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States."

(b) Clerical Amendment.—The table of chapters for part II of title 18 of the United States Code is amended by inserting after the item relating to chapter 205 the following new item:

"206. Pen Registers .... 3121".

SEC. 302. EFFECTIVE DATE.

(a) In General.—Except as provided in subsection (b), this title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) Special Rule for State Authorizations of Interceptions.—Any pen register order or installation which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such order or installation occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of changes in State law required in order to make orders or installations under Federal law as amended by this title; or

(2) the date two years after the date of the enactment of this Act.

Purpose

The purpose of the legislation is to amend title 18 of the United States Code to prohibit the interception of certain electronic communications; to provide procedures for interception of electronic communications by federal law enforcement officers; to provide procedures for access to communications records by federal law enforcement officers; to provide procedures for federal law enforcement access to electronically stored communications; and to ease certain procedural requirements for interception of wire communications by federal law enforcement officers.

History

When the Framers of the Constitution acted to guard against the arbitrary use of government power to maintain surveillance over citizens, there were limited methods of intrusion into the "houses, papers and effects" protected by the Fourth Amendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions.

The telephone is the most obvious example. Its widespread use made it technologically possible to intercept the communications of citizens without entering homes or other private places. When the issue of government wiretapping first came before the Supreme Court in *Olmstead* v. *United States*, 277 U.S. 438, the Court held that wiretapping did not violate the Fourth Amendment, since

17

there was no searching, no seizure of anything tangible, and no physical trespass.[1]

But the *Olmstead* case is remembered not only for its holding but for the prescient dissent of Mr. Justice Brandeis, who predicted:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . Can it be that the Constitution affords no protection against such invasions of individual security?[2]

Forty years later, the Supreme Court accepted the logic of Justice Brandeis in *Katz* v. *United States*, 389 U.S. 347 (1967), holding that the Fourth Amendment applies to government interception of a telephone conversation. At the same time, the Court extended Fourth Amendment protection to electronic eavesdropping on oral conversations in *Berger* v. *New York*, 388 U.S. 41 (1967).

Congress responded in a comprehensive fashion by authorizing government interception, under carefully subscribed circumstances, in Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[3] which has come to be known as the Wiretap Act. That legislation protected two common types of communication—telephone conversations and face-to-face oral communications—against electronic eavesdropping. Specifically, the law barred the interception of wire communications over a common carrier unless an appropriate court order had been obtained.[4] Further, it limited the concept of interception to the "aural acquisition" of the contents of a communication.[5] "Oral communications" were protected only in circumstances where there is a reasonable expectation of privacy.[6]

Nature of the Problem

Although it is still not twenty years old, the Wiretap Act was written in different technological and regulatory era. Communications were almost exclusively in the form of transmission of the human voice over common carrier networks. Moreover, the contents of a traditional telephone call disappeared once the words transmitted were spoken and there were no records kept. Consequently the law primarily protects against the aural interception of the human voice over common carrier networks.

The legislation did not attempt to address the interception of text, digital or machine communication.[7] This statutory framework appears to leave unprotected an important sector of the new communications technologies.

Many communications today are carried on or through systems which are not common carriers. Electronic mail, videotex and similar services are not common carrier services. Under existing law

[1] Olmstead v. United States, 277 U.S. 438, 464 (1928). *Compare* Dow Chemical Co. v. United States, — U.S. — (May 19, 1986) (aerial photography by government without a warrant does not violate Fourth Amendment); California v. Ciraolo, — U.S. — (May 19, 1986) (same).
[2] 277 U.S. at 474 (Brandeis, J., dissenting).
[3] 18 U.S.C. 2510 *et seq.* hereinafter "Wiretap Act."
[4] 18 U.S.C. 2511.
[5] 18 U.S.C. 2510.
[6] *Id.*
[7] Sen. Rep. No. 1097, 90th Cong., 2d Sess. 90, hereinafter "1968 Senate Report."

the interception of these services or the disclosure of the contents of messages over these services are probably not regulated or restricted. Moreover, totally private systems are rapidly being developed by private companies for their own use. It is not uncommon for businesses now not to use the local telephone comapny in some instances the long distance companies in the creation of voice and data networks. Since these networks are private they are not covered by existing Federal law. In addition, data is transmitted over tradional telephone services as well as by these services. Since data, unlike the human voice, cannot be aurally intercepted, it is also largely unregulated and unrestricted under present law.

Today, we have large-scale electronic mail operations, cellular and cordless telephones, paging devices, miniaturized transmitters for radio surveillance, and a dazzling array of digitized information networks which were little more than concepts two decades ago. Unfortunately, the same technologies that hold such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the government.

In 1984 the Federal government engaged in more telephone surveillance and wiretapping than in any year since 1973.[8] Moreover, according to a recent study by the Office of Technology Assessment, Federal agencies are planning to use or already use radio scanners (20 agencies), cellular telephone interception (6 agencies), tracking devices (15 agencies), pen registers (14 agencies), and electronic mail interceptions (6 agencies).[9]

This increased use of a variety of electronic surveillance devices alone is not cause for alarm. There are instances when a particular electronic surveillance technique is justified in a criminal investigation. Congress has recognized this by permitting—under carefully limited circumstance under the Wiretap Act—the tapping of telephone calls or the bugging of rooms. However, despite efforts by both Congress[10] and the courts,[11] legal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology.

The statutory deficiency in Title III with respect to non-voice communications has been criticized by commentators, Congressional experts, and most recently by both the General Accounting Office and the Office of Technology Assessment.[12] The danger is eloquently pointed out by Professor Richard Posner (now United States Circuit Court Judge):

[8] Administrative Office of the United States Courts, *Report on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications (Wiretap Report) for the Period January 1, 1984 to December 31, 1984*.

[9] Office of Technology Assessment, U.S. Cong., Electronic Surveillance and Civil Liberties (1985), hereinafter "OTA Report."

[10] *E.g.*, The Wiretap Act, supra note 3, Foreign Intelligence Surveillance Act, 50 U.S.C. 1801 et seq., Right to Financial Privacy Act, 12 U.S.C. 3401 et seq.

[11] *E.g.*, United States v. Torres, 751 F.2d 875 (7th Cir. 1984) cert. den'd, —U.S.—, 105 S.Ct. 1853 (1985) (court has authority to issue warrant permitting video surveillance); Katz v. United States, 389 U.S. 347 (1967) (Fourth Amendment applies to government wiretapping of telephone conversations); Berger v. New York, 388 U.S. 41 (1967) (Fourth Amendment applies to electronic eavesdropping on oral conversations).

[12] *See generally*, *Electronic Communications Privacy Act of 1985: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the House Comm. on the Judiciary*, 99th Cong., 1st and 2d Sess., hereinafter "House Hearings." *See also* Burnham, *Ex-perts Study Effect on Law of Latest Electronic Services*, N.Y. Times, Mar. 18, 1985 (reporting on study by ACLU Project on Privacy and Technology).

In the absence of market discipline, there is no presumption that the government will strike an appropriate balance between disclosure and confidentiality. And the enormous power of the government makes the potential consequences of its snooping far more ominous than those of . . . a private individual or firm.[13]

This legal uncertainty poses potential problems in a number of areas. First, it may unnecessarily discourage potential customers form using such systems, and encourage unauthorized users to obtain access to communications to which they are not party.[14] Lack of clear standards may also expose law enforcement officers to liability[15] and endanger the admissibility of evidence.[16]

But most important, if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right.[17] Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.[18] Additional legal protection is necessary to ensure the continued vitality of the Fourth Amendment.[19]

The Committee believes the bill represents a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement.

Telecommunications Technologies Under Current Law

Radio Telephones

When Congress passed the Wiretap Act in 1968, most telephone calls were transmitted as they always had been—by wire. Other technologies, however, were already on the horizon, an inevitability implicitly recognized by Congress in protecting telephone calls carried "in whole or in part" over wire. 18 U.S.C. 2510. Today, only a minority of telephone calls are made through wire alone; the majority combine wire with some form of radio technology, usually microwave.

a. Microwave

Microwave consists of extremely high frequency radio waves transmitted point-to-point on line-of-sight paths between antennas located on towers or building tops (in terrestrial microwave systems) and between satellites and earth station "dish" antennas (in satellite-based systems). Like most radio transmissions, the microwave portion of a telephone call is vulnerable to interception.[20]

[13] Posner, *Privacy in the Supreme Court*, 1979 Sup. Ct. Rev. 173, 176 (1979).

[14] House hearings, supra note 12 (testimony of P. Walker, P. Quigley, P. Nugent, J. Stanton et al.)

[15] *See* Malley v. Briggs, —U.S.— (84-1586, Mar. 5, 1986), 54 U.S.L.W. 4246 (Mar. 5, 1986).

[16] 18 U.S.C. 2515.

[17] According to a recent poll, 77 percent of Americans are concerned about technology's threats to their personal privacy. Louis Harris & Associates, *The Road After 1984*, Southern New England Telephone (1984).

[18] *See* Dow Chemical v. United States, — US — (May 19, 1986) (Powell, J. dissenting).

[19] For recent explorations on the capacity of Congress to interpret the Constitution see Mikva, *How Well Does Congress Support and Defend the Constitution?*, 61 N.C. L. Rev. 587 (1983); Fisher, *Constitutional Interpretation by Members of Congress*, 63 N.C. L. Rev. 707 (1985).

[20] T. Harrington and B. Cooper, The Hidden Signals on Satellite TV (1984).

The equipment to complete an interception can be expensive, and the task difficult; however, the practice is sufficiently well known as to be an option for satellite dish owners and for foreign intelligence agencies. Despite the availability of the technical means of interception of microwave transmissions, such transmissions are protected by the plain language of Title III.

b. Cellular Telephone

In 1981 the Federal Communications Commission approved the use of cellular telephone services.[21] This technology uses both radio transmissions and wire to make "portable" telephone service available in a car, a briefcase, or in rural areas not reached by telephone wire.

In a cellular radiotelephone system, large service areas are divided into honeycomb-shaped segments or "cells"—each of which is equipped with a low-power transmitter or base station which can receive and radiate messages within its parameters. When a caller dials a number on a cellular telephone, a transceiver sends signals over the air on a radio frequency to a cell site. From there the signal travels over phone lines or a microwave to a computerized mobile telephone switching office ("MTSO") or station. The MTSO automatically and inaudibly switches the conversation from one base station and one frequency to another as the portable telephone, typically in a motor vehicle, moves from cell to cell.[22]

Cellular technology, because it is more complex, is more difficult to intercept than traditional mobile telephones; it is, however, more accessible than microwave transmissions. Cellular telephone calls can be intercepted by either sophisticated scanners designed for that purpose, or by regular radio scanners modified to intercept cellular calls.[23]

The availability of this technology poses a troubling conflict between the technology of surveillance and new techniques of communication using radio. Interception of cellular calls is illegal under current federal law.[24] At least one state has passed a law specifically aimed at protecting cellular calls.[25] Notwithstanding

[21] Cellular Communications Systems Decisions, 86 FCC 2d 469 (1981).

[22] House Hearings, supra note 12, testimony of P. Quigley, J. Stanton. Cellular technology is more advanced than ordinary mobile telephones. Cell-to-cell "hand-off" of calls maximizes channel capacity, allowing use by many more subscribers in a specific area. In addition, cellular telephone calls are fully automated and do not require the services of a mobile operator.

[23] *House Hearings*, supra, note 12 (testimony of R. Colgan); see Ad, Land Mobile Product News, Jan. 15, 1985 (for Regency scanners). When cellular service began it was "remarkably private." Huff, *Cellular Phone*, Technology Review (Nov./Dec. 1983) at 53, 56. This was so because unlike older radio telephones there is usually no operator required to place the calls, and there is no party line function. Greenhouse, *Privacy and the Cellular Phone*, Personal Communications Magazine. In addition, because cellular was assigned to new frequencies (between 825 Mhz and 890 Mhz), scanners were not initially available to easily enable scanning of cellular calls by the general public. *Id.* More recently, such scanners have been made available for sale. Hanson, *Legislating Cellular Privacy: An Idea That Won't Work*, Personal Communications Magazine; Corn, *The Privacy Issue*, Cellular Resources, 66, 71 (Sept./Oct. 1984); Corn, *The Privacy Issue Updated*, Cellular Resources 46-49 (Nov. 1985).

[24] *See* House Hearings, supra n. 12 (testimony of U.S. Dept. of Just.) (interception of cellular to landline calls illegal because "in whole or in part by wire" 18 U.S.C. 2510); *cf.* United States v. Hall, 488 F.2d 193 (9th Cir. 1973) (same for ordinary mobile telephones); 47 U.S.C. 705 (interception and divulgence or use of communications not broadcast for general public illegal). Perhaps because of the relative newness of the technology, there are no cases directly addressing the issue of cellular interceptions.

[25] Cal. Penal Code §632 et seq.

these legal proscriptions there remains a real-life conflict as interception technology catches up with communications development.[26] The resolution of these competing interests was carefully considered by the Committee.

c. Cordless Telephones

Cordless telephones are another new telephone technology presenting a conflict between communication and interception. A cordless telephone consists of a handset and a base unit wired to a landline and a household/business electrical current. A communication is transmitted from the handset to the base unit by AM or FM radio signals. From the base unit the communication is transmitted over wire, the same as a regular telephone call. The radio portions of these telephone calls can be intercepted with relative ease using standard AM radios.[27]

The legality of intercepting cordless telephone calls has been fully litigated in only two states. The Supreme Courts of Kansas and Rhode Island, both construing federal law, have held that evidence obtained by an interception of a cordless telephone call by law enforcement officials without a warrant can be admitted at trial.[28] In each case the court was convinced that the radio portion of a conversation was entitled to no legal protection against interception.[29] This approach sharply conflicts with the major relevant federal case.[30]

These courts were not required, however, to decide the rights of the other party to the conversations in these cases, persons using conventional landline telephones. While it it possible to argue that a person using a cordless phone knows or has reason to know that the call can be easily overheard, that argument does not apply to the other party to the conversation.

Data Transmissions and Electronic Mail

When Congress enacted the Wiretap Act it specifically excluded the transmission of data from protection against private and governmental interceptions.[31] In the intervening years, data transmission and computer systems have become a pervasive part of the business and home environments.

Computer and telephone technologies have merged; the resulting new communication techniques utilize computer terminals and

[26] House Hearings, supra note 12 (testimony of R. Colgan). The wide availability of this technology and its expanded use of up to 7 million such phones by 1990, poses additional challenges to law makers.

[27] *See* State v. DeLaurier, 488 A.2d 688 (R.I. 1985); State v. Howard, 235 Kan. 236, 679 P.2d 197 (1984).

[28] 488 A.2d 688, 235 Kan. 236, 679 P.2d 197.

[29] 488 A.2d 688, 235 Kan. 236, 679 P.2d 197. The state courts concluded that radio communications are neither "wire" nor protected "oral communications". 488 A.2d at 693, 235 Kan. at 2[illegible]. They reasoned that to require the police to obtain a warrant to listen to an AM radio would be "absurd". 488 A.2d at 694. They also reasoned that such communications were not protected against interception because there is no "reasonable expectation of privacy". State v. DeLaurier, 488 A.2d at 694; State v. Howard, 235 Kan. 236, 679 P.2d 197 (1984). The *DeLaurier* court also found that an AM radio is not a "device" within the meaning of 18 U.S.C. 2510(5), therefore no violation of federal law occurred. 488 A.2d at 694.

[30] United States v. Hall, 488 F.2d 193 (9th Cir. 1973) (interception of radio portion of mobile telephone call violates Wiretap Act since communication "in whole or in part by wire". 18 U.S.C. 2510).

[31] 1968 Senate Report, supra note 7, at 90.

video display screens, and frequently transmit data over telephone lines.

The array of services include electronic bulletin boards, electronic data bases, videotext services, and remote computing. Some of these new services permit an individual to use a keyboard and telephone to transmit electronic messages and data and to receive interactive services featuring banking and other financial services, shopping, news, messages, and education. Many of these services also record the nature of the transactions engaged in by the user. Thus, the new technologies represent both an explosion in communication opportunities as well as surveillance possibilities.[32]

One of the most popular new computer services is electronic mail, a service which combines features of the telephone and regular first class mail. Electronic mail can include telex, teletex, facsimile, voice mail and mixed systems that electronically transmit and store messages. Many e-mail users have found it a useful substitute for telephone calls, while others utilize it instead of the government postal service.

Electronic mail differs from regular mail in three ways. First, e-mail is provided by private parties and thus not subject to governmental control or regulation under the postal laws.[33] Second, it is interactive in nature and can involve virtually instantaneous "conversations" more like a telephone call than mail. Finally, e-mail is different from regular mail because the electronic communication provider as part of the service may technically have access to the contents of the message and may retain copies of transmissions.[34]

Any discussion of the application of current law governing interception of e-mail or the use of e-mail surveillance begins with the Fourth Amendment, which protects our reasonable expectation of privacy. There are no reported cases governing the acquisition of e-mail by the government, so an application of the Fourth Amendment to the interception of e-mail is speculative. It appears likely, however, that the courts would find that the parties to an e-mail transmission have a "reasonable expectation of privacy" and that a warrant of some kind is required.

As for statutory protection, while there may be some limits on government access to e-mail messages from an e-mail provider, there do not appear to be any federal statutes which directly address this issue.[35] Title III would not apply, since it is limited to the "aural acquisition" of the contents of a communication, and e-mail usually does not involve the transmission of audible sound.[36] The Communications Act might have some limited application, excepting law enforcement officials.[37] The Foreign Intelligence Sur-

[32] OTA Report, supra note 9, at 48.

[33] See 18 USC 1701 et seq. These regulations appear to place restrictions on government access to government operated electronic mail systems. Although the United States Postal Service operated an electronic mail system for a short period, that service is no longer in operation.

[34] House Hearings, supra note 11 (testimony of P. Walker). E-mail systems are designed to provide access to contents and copies of messages in case of system failure. Messages are electronically preserved and not normally accessed by the e-mail provider.

[35] The Right to Financial Privacy Act may apply if certain categories of records are involved. 12 USC 3401 et seq.

[36] See 18 USC 2510; United States v. New York Telephone Company, 434 U.S. 159, 166 (1977).

[37] 47 USC 705 [illegible] the interception and disclosure or use of certain communications, applies only to radio or wire communications. Some courts have held that the statute does not

Continued

veillance Act, however, could be read to require federal law enforcement officials to obtain a court order before engaging in "electronic surveillance" that acquires the contents of e-mail communications.[38] These criminal prohibitions do not apply to private persons.

REMOTE COMPUTING SERVICES

The use of remote computing services has also dramatically increased.[39] Many persons use the facilities of these services to process and store their own data.

A subscriber or customer to a remote computing service transmits records to a third party, a service provider, for the purpose of computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer.

As with electronic mail, remote computing services are still relatively new, and there is no case law directly on point. Proceeding by analogy, under current law a subscriber or customer probably has very limited rights to assert in connection with the disclosure of records held or maintained by remote computing services.[40] It is likely, however, that contents of customer data enjoy a higher degree of Fourth Amendment protection.[41]

PAGING DEVICES

An increasingly important adjunct to the telecommunications systems is the paging system. Radio paging is essentially a one-way message service. Recent estimates indicate that there are over 2.5 million pagers in operation; these numbers are expected to double within five years.[42]

There are three basic types of paging devices: tone-only, digital, and voice.[43] In a tone-only pager system an outside party places a telephone call to the paging service which in turn sends a signal to the user indicating that the user has a telephone call. The user must then call back a specific phone number (often an answering service). The digital or display pager permits the user to receive a

govern the activities of law enforcement officials. United States v. Hall, 488 F.2d 193, 197 (9th Cir. 1973); United States v. Christman, 375 F. Supp. 1354 (N.D. Cal. 1974).

[38] 50 USC 1809(a) provides that it is a felony for a person to "engage in electronic surveillance under color of law except as authorized by statute." 50 USC 1801(f) includes within the definition of "electronic surveillance" "the acquisition ... of the contents of any wire or radio communication ..." 50 USC 1801(f).

[39] House Hearings, supra note 12 (testimony of P. Nugent).

[40] Cf. United States v. Miller, 425 U.S. 435 (1976) (no standing under Fourth Amendment for customer to object to bank disclosure of customer records). Congress reversed the result reached in Miller by enacting the Right to Financial Privacy Act, 12 USC 3401 et seq.

[41] Miller, note 39 supra, might be distinguished when contents rather than records are involved. Unlike records of the bank's (or remote computing service's) records, contents are analogous to items stored, under the customer's control, in a safety deposit box.

[42] According to one consultant for Arthur D. Little, the number of pagers in service would grow to 10 million (including 6 million display pagers) by 1990. Telocator Members Tout The Paging to Prosper in the Future, TELOCATOR BULLETIN, September, 1984.

[43] See generally, Note, Does A Part Equal the Whole: Is the Interception of Paging Device Communications Governed by Title III, 7 Geo. Mason U.L. Rev. 234 (1984). Newer two-way paging devices are apparently on the horizon. [illegible], Radio Pagers Expand Horizons, HIGH TECHNOLOGY (March 1985).

digital or alphanumeric message on a display screen. A voice pager permits a person who wishes to communicate with the user to leave a recorded message which is then transmitted to the user. The user actually hears the voice message.

The only reported case on this technology, Dorsey v. State,[44] involves a voice pager. In the Dorsey case, the court upheld the use of a scanner by the police to intercept voice messages transmitted over a paging system to an alleged drug dealer. The court held that these messages are neither wire nor oral communications and, therefore, such interceptions are lawful.[45]

According to the United States Department of Justice, however, the three types of paging devices require different levels of statutory protection.[46] The Department reasons that "tone only" pagers carry no reasonable expectation of privacy and therefore no court order is required for a government official to intercept or monitor such signals. The interception of "display pagers" is, according to the Department of Justice, also not within the ambit of Title III; the Department concedes, however, that because use of such devices encompasses a reasonable expectation of privacy, governmental interception of messages over such a system requires use of a search warrant under the Fourth Amendment.[47] Finally, the Department of Justice concludes that a "voice pager" is simply the continuation of an original wire communication, and therefore a Title III court order is required.[48]

PEN REGISTERS

The privacy of telephone customers can also be affected by the use of pen registers or other devices which record the numbers dialed from a telephone.[49] Pen registers can be used by telephone companies for internal business purposes[50] as well as by the government for law enforcement purposes.[51] It is thus governmental use which has posed the most difficult questions for Congress and the courts.[52]

[44] 402 So. 2d 1178 (Fla. 1981). In Dorsey, the Supreme Court of Florida interpreted a state statute in pari materia with Federal law. 402 So. 2d at 1183.

[45] Id. The Dorsey court specifically rejected the reasoning in United States v. Hall, 488 F.2d 193 (9th Cir. 1973).

[46] U.S. Department of Justice, Office of Legal Counsel (Theodore B. Olson), Memorandum for John A. Mintz, Assistant Director-Legal Counsel, Federal Bureau of Investigation, January 3, 1984 (Olson Memo).

[47] Olson Memo, Supra note 46.

[48] Id. Compare Dorsey v. State, 402 So. 2d 1178 (Fla. 1981).

[49] See United States v. N.Y. Tel. Co., 434 U.S. 159, 161, 167 (1977); United States v. Giordano, 416 U.S. 505, 549 n. 1 (1974) (Powell, J., concurring in part and dissenting in part).

[50] Telephone companies can use pen registers to verify long distance billing information. Fishman, Pen Registers and Privacy: Risks, Expectations and the Nullification of Congressional Intent, 29 CATHOLIC L. REV. 557, 558 (1980). Telephone companies can use pen registers to detect the use of illegal devices such as "blue boxes." United States v. N.Y. Tel. Co. 434 U.S. 159, 174-75 (1977). See generally Note, The Legal Constraints Upon the Use of the Pen Register as a Law Enforcement Tool, 60 CORNELL L. REV. 1028, 1029 (1975). Additionally, a pen register could be placed on the phone of a person suspected of placing harrassing or obscene calls. 47 U.S.C. 223. See generally Claerhout, The Pen Register, 20 DRAKE L. REV. 108, 109-10 (1970).

[51] Pen registers are often used to acquire "probable cause" evidence necessary to obtain a search warrant or a Title III wiretap order. House Hearings, supra note 12 (testimony of J. Keeney, Remarks, [illegible], Criminal Division, United States Department of Justice, Office of Technology Assessment Workshop, May 17, 1985. See also Fishman, WIRETAPPING AND EAVESDROPPING 66 (1978).

[52] Slightly different issues are presented when law enforcement officials utilize devices which stop or trace [illegible] phone calls. Prior to the passage of Title III courts had upheld the use of

Continued

The United States Supreme Court has on two occasions decided cases involving questions about the legality of installation and use of pen registers. United States v. N.Y. Tel. Co.[53] presented the question whether an ordinary search warrant was sufficient to authorize government use of a pen register. The Court held that the existing federal wiretap law was not implicated by the use of a pen register,[54] and that federal district judges have authority to issue warrants directing telephone company cooperation with the installation of pen registers.[55]

In Smith v. Maryland[56] the Supreme Court found that law enforcement officials need not obtain a search warrant before securing telephone company cooperation in the installation of a pen register.[57] The Court reasoned that because the person who used the telephone voluntarily disclosed the numbers dialed there was "no reasonable expectation of privacy," eliminating Fourth Amendment protection.[58]

The current practice of federal law enforcement agencies is to obtain a court order, under Rule 57 of the Federal Rules of Criminal Procedures,[59] before using a pen register.[60] This practice conforms with the Foreign Intelligence Surveillance Act,[61] which created a requirement for a court order even in a domestic criminal case.[62] Outside the limited context of foreign intelligence, Congress has specified no standard for obtaining a pen register court order. Thus, current case law and statutes leave federal law enforcement officials with virtually unchecked discretion to obtain information through the use of pen registers. All the government needs to do is make an application to a federal court; no independent judicial review of the facts is required.

RECORDS

Electronic communication technologies have become so pervasive that extensive records are maintained which reveal a great deal about how individuals interact with each other. For decades, telephone companies have maintained telephone toll records and tele-

such devices because of the consent of one of the parties to the communication. Rathbun v. United States, 355 U.S. 107 (1957). Enactment of Title III has not affected this result. Carr, THE LAW OF ELECTRONIC SURVEILLANCE, § 3.08(2) at 84 (1977) and at 23 (1986 Supp.).

[53] 434 U.S. 159 (1977).

[54] Id. at 165–68.

[55] Id. at 171–78.

[56] 442 U.S. 735 (1979).

[57] Id. at 746.

[58] Id. at 745.

[59] The Rule specifies: In all cases not provided for by rule, the district judges and magistrates may regulate their practice in any manner not inconsistent with these rules or those of the district in which they act. FED. R. CRIM. PROC. 57.

[60] The Subcommittee on Courts, Civil Liberties and the Administration of Justice of the Committee on the Judiciary, United States House of Representatives, conducted a survey of all [illegible] federal district court Chief Judges to ascertain how frequently pen registers are used. The Subcommittee received 60 responses which indicated that for these courts 2,199 pen register orders were obtained during the first 9 months of 1985.

[61] Public Law 95-511, 50 U.S.C. 1801 et seq.

[62] 50 U.S.C. 1809 creates criminal liability for federal officials who engage in electronic surveillance, unless such official has either a search warrant or a court order from a court of competent jurisdiction. 50 U.S.C. 1801(f) defines "electronic surveillance" to include the acquisition of the "contents" of wire communications and further defines "contents" to "include any information concerning the identity of the parties to such communication or the existence, substance, purport or meaning of that communication." Thus, the Foreign Intelligence Surveillance Act covers the use of pen registers. H.R. Rep. No. 1283, 95th Cong. 2d Sess. 67 (1978).

graph companies have kept copies of telegrams. There is a body of law which addresses the question of government access to this data.[63] Similarly there are legal rules which limit the access to information about postal correspondence.[64]

The newer technologies such as electronic mail and remote computing services maintain a type of records which do not neatly fit within the legal categories which exist for older technologies. This legal uncertainty has caused concern within the business community for several reasons. First, to the extent that potential customers have less protection when they use an electronic medium than with paper, there may be a disincentive to use an electronic service.[65] Second, if persons with records have a choice of maintaining them "in house" or with a third party, they may be less inclined to go outside if such a move deprives them of legal rights (such as notice and an opportunity to contest government access). Any effort to resolve this legal uncertainty should first proceed from a complete understanding of the existing law with respect to more traditional technologies.

Telephone toll records

As a general matter telephone companies maintain a record of calls placed from a telephone for billing purposes. These business records are primarily used by the telephone company for its own purposes. At the federal level the government can legally obtain access to such records based on a grand jury or trial subpoena or through the use of an administrative summons authorizing a specific federal agency to obtain records.[66] Such government access is usually in connection with an ongoing criminal or civil investigation.[67] The most frequent use of this investigative technique is by the Department of Justice.[68] Requests for telephone toll records would appear to easily exceed 100,000 per year.[69]

At the state level, some states have placed limits on access to telephone toll records by state and local law enforcement. Colora-

[63] *See generally* Reporters Committee v. AT&T 593 F.2d 1030 (D.C. Cir. 1978), cert. denied, 440 U.S. 949 (1979) (no violation of the Fourth Amendment to release toll call records without notice to the customer); *see also* Smith v. Maryland 442 U.S. 735 (1979) (use of a "pen register" is permissible under Fourth Amendment because a subscriber has no reasonable expectation of privacy in numbers dialed).

[64] 39 U.S.C. 3623(d) (requires search warrant to open first class mail); United States v. Van Leeuwen, 397 U.S. 249 (1970) (first class mail may only be opened pursuant to warrant under Fourth Amendment); Ex parte Jackson, 96 U.S. 727, 733 (1878) ("whilst in the mail ... [letters] ... can only be opened and examined under ... warrant").

The use of mail covers, which record the names and addresses of senders and recipients of mail, have different legal standards applied to their use. Because investigative use of the information does not include access to the contents of the letter there has been a lesser degree of Fourth Amendment concern. *See* note 2, *infra*.

[65] *See* House Hearings, *supra* note 12, testimony of M. Nugent.

[66] Reporters Comm. v. AT&T, *supra* note 61.

[67] *Id.*

[68] *Id.*

[69] The Committee conducted a survey of various telephone companies to ascertain the frequency with which telephone toll records are sought. For approximately six states (Maryland, Washington, D.C., Colorado, Michigan, Illinois and most of California) nearly 10,000 subpoenas were issued by the Department of Justice for a one year time period. NYNEX reported that for New York State alone, subpoenas were received relating to between 85,000 and 91,000 telephones per year over the past five years.

In Reporters Comm. v. AT&T, *supra*, note 61, at 1037, it was estimated that the number of requests for telephone toll records was at a rate of between two and three thousand each month.

do,[70] California,[71] Pennsylvania,[72] and New Jersey,[73] have all required that a court order be obtained before access to telephone-created transactional information can be granted. The majority view, however, appears to conform with federal law, that is to permit access based on any form of legal process.[74]

Telegrams

The applicable federal law would appear to permit governmental access to copies of telegrams based on the use of a subpoena.[75]

First class mail searches and mail covers

One of the most frequently used forms of private communication is the government operated first class mail system. Therefore, an assessment of the limitations which have been placed on governmental access to the contents of and/or transactional information concerning first class mail correspondence is relevant to any determination about what legal rights should exist with respect to access by the government to newer forms of communications.

Under current Federal law, a search warrant based on probable cause is required before the government can obtain the contents of a first class letter.[76]

A lower standard is used for government access to mail covers, an investigative technique whereby the postal service records the names and addresses of persons who write to an investigative target or to whom such person writes. While the United States Postal Service does place limits (by regulation) on the use of this technique, courts have thus far declined to find a Fourth Amendment interest implicated by the practice.[77]

STATEMENT

Legislation amending the Wiretap Act to include new technologies, H.R. 214, was first introduced in the 95th Congress by Congressman Robert W. Kastenmeier, Chairman of the Subcommittee on Courts, Civil Liberties and the Administration of Justice of the

[70] People v. Sporleder, 666 P.2d 135 (Sup. Ct. Colo. 1983); Charnes v. diGiacomo, 612 P.2d 1117 (Sup. Ct. Colo. 1980); People v. Corr, 682 P.2d 20 (Sup. Ct. Colo. 1984).

[71] People v. Blair, 25 Cal. 3d 640, 602 P.2d 738 (Calif. Sup. Ct. 1979); People v. McKunes, 124 Cal. Rep. 126 (Calif. Ct. App. 1975).

[72] Commonwealth v. DeJohn, 486 Pa. 32, 403 A.2d 1283 (1979), Cert. denied 444 U.S. 1032 (1980).

[73] State v. Hunt, 91 N.J. 338, 450 A.2d 952 (1982); Note, 13 Seton Hall L. Rev. 602 (1983).

[74] In re Order for Indiana Bell Telephone to Disclose Records 409 N.E. 2d 1089 (Sup. Ct. Ind. 1980); State v. Fredette, 411 A.2d 65 (Sup. Ct. Me. 1979); Hanson v. Bohan, 639 P.2d 10 (Sup. Ct. Montana 1982); People v. DiRaffaele, 55 N.Y. 2d 234, 433 N.E. 513 (Ct. App. 1981); Fitzgerald v. State, 599 P.2d 572, 577 (Sup. Ct. Wyo. 1979).

[75] Wheeler v. United States, 226 U.S. 478 (1913) (a subpoena requiring production of telegrams upheld against a Fourth Amendment challenge); *see also* Brown v. United States, 276 U.S. 134 (1928) (upholding finding of criminal contempt against person who refused to comply with subpoena of copies of telegrams).

[76] *See* note 64, *supra*.

[77] 39 C.F.R. 233.2; United States v. Krauth, 769 F.2d 473 (8th Cir. 1985); United States v. Gering, 716 F.2d 615 (9th Cir. 1983); United States v. Depoli, 628 F.2d 779 (1980); United States v. Huie, 593 F.2d 14 (5th Cir. 1979); United States v. Choate, 576 F.2d 165 (1978), and 619 F.2d 21 (9th Cir. 1980); Vreeken v. Davis, 718 F.2d 343 (10th Cir. 1983); *see also* Paton v. LaPrade, 469 F.Supp. 773 (D.N.J. 1978). *See generally* Burnham, *Keeping an Eye on Suspects' Mail*, New York Times, March 1, 1986, pg. B-10.

House Committee on the Judiciary. That legislation grew out of widespread general concern with government surveillance.[78]

Although H.R. 214 was not enacted, Congressman Kastenmeier revisited the subject in general oversight hearings held in the 98th Congress entitled "1984: Civil Liberties and the National Security State." [79]

As a result of those hearings, a bill, H.R. 6343, was introduced in the 98th Congress by Congressman Kastenmeier that served as a model for legislation in the 99th Congress.

During the 99th Congress, the Committee, acting through the subcommittee on Courts, Civil Liberties, and the Administration of Justice—held four days of hearings on H.R. 3378 the bill on which H.R. 4952 is based, introduced by Chairman Kastenmeier and Cong. Carlos J. Moorhead, ranking minority Member of the Subcommittee. An identical bill, S. 1667, was introduced in the Senate by Sen. Patrick J. Leahy, ranking minority Member of the Subcommittee on Patents, Copyrights and Trademarks of the Senate Committee on the Judiciary, and Sen. Charles McC. Mathias, Chairman of the Subcommittee.

On September 26, 1985, the Subcommittee heard from the following witnesses: Senator Patrick Leahy (United States Senator from Vermont); Philip M. Walker (general regulatory counsel, GTE Telenet Inc., on behalf of the Electronic Mail Association); and Philip J. Quigley (president and chief executive officer, Pactel Mobile Companies, on behalf of the Cellular Telecommunications Industry Association).

On October 24, 1985, the subcommittee heard from Fred W. Weingarten (program manager, communication and technologies program, Office of Technology Assessment, United States Congress); P. Michael Nugent (government affairs counsel, Electronic Data Systems Corporation, on behalf of ADAPSO, the computer software and services industry association), and John Stanton (executive vice president, McCaw Communications Companies, Inc., on behalf of Telocator Network of America).

On January 30, 1986, the subcommittee took testimony from Neal Amick (division manager for corporate security, American Telephone and Telegraph Company); John W. Kelly Jr. (attorney, Southwestern Bell Telephone Company); Perry Williams (secretary, American Radio Relay League, Inc., a group representing ham radio operators, presenting the statement of Dr. Larry E. Price, president of the group); George A. Kuhnreich, (vice president for corporate planning and governmental affairs, Tandy Corporation); and Richard T. Colgan (executive secretary, Association of North American Radio Clubs).

On March 5, 1986, the final day of hearings, the witnesses were James I. K. Knapp (Deputy Assistant Attorney General, Criminal Division, United States Department of Justice); and Clifford F. Fishman (Professor of Law, Columbus School of Law, Catholic University of America, and author of *Wiretapping and Eavesdropping*.

[78] *See generally Surveillance, Hearings on the Matter of Wiretapping, Electronic Eavesdropping and Other Surveillance Before the Subcommittee on Courts, Civil Liberties and the Administration of Justice of the House Comm. on the Judiciary*, 94th Cong., 1st Sess.

[79] *1984: Civil Liberties and the National Security State Hearings Before the Subcommittee on Courts, Civil Liberties and the Administration of Justice*, 98th Cong., 1st and 2d Sess. 133-256.

The Subcommittee took note that the Senate held a hearing on S. 1667, on November 13, 1985.

After completion of the hearing process in the 99th Congress, H.R. 3378, the bill on which H.R. 4952 is based, went to subcommittee mark-up on May 14, 1986. Two amendments, offered by Mr. DeWine, were not accepted by the subcommittee. A quorum of Members being present, the bill, as amended by Chairman Kastenmeier by an amendment in the nature of a substitute, was passed by a voice vote and reported in the form of a clean bill H.R. 4952 was introduced by Mr. Kastenmeier on June 5, 1986, cosponsored by 14 Members of the subcommittee and 10 other Members: Mr. Moorhead, Mr. Brooks, Mr. Mazzoli, Mr. Synar, Mrs. Schroeder, Mr. Frank, Mr. Morrison of Connecticut, Mr. Berman, Mr. Bouncher, Mr. Hyde, Mr. Kindness, Mr. Swindall, Mr. Coble, Mr. Edwards of California, Mr. Conyers, Mr. English, Mr. Matsui, Mr. Bruce, Mr. Owens, Mr. Mitchell, Mr. Kostmayer, Mr. Nowak, and Mr. Leland.

On June 10, 1986, the full Committee considered H.R. 4952 and, after general debate, and without substantive amendment, ordered the bill reported favorably by roll call vote, 34-0, a quorum of Members being present.

SUPPORT FOR THE LEGISLATION

The organizations and individual corporations named below support the principles embodied in the legislation.

Organizations

Electronic Mail Association
ADAPSO (Computer software and services industry association)
Telocator Network of America
Cellular Telecommunications Industry Association (CTIA)
American Civil Liberties Union (ACLU)
National Association of Manufacturers (NAM)
U.S. Chamber of Commerce
National Association of Broadcasters (NAB)
National Cable Television Association (NCTA)
National Association of Business & Educational Radio (NABER)
American Radio Relay League (ham operators)
CBEMA (Computer and Business Equipment Manufacturers Association)
U.S. Telephone Association
Videotext Industry Association
Information Industry Association
Electronic Funds Transfer Association
Radio and Television News Directors Association
Association of American Railroads
Institute of Electrical and Electronics Engineers (IEEE)
Direct Marketing Association
Utilities Telecommunications Council
Associated Credit Bureaus, Inc.

Corporations

AT&T
General Electric
IBM
GTE
ITT
MCI
CBS
Capital Cities/ABC, Inc.
National Broadcasting Co., Inc. (NBC)
Tandy Corporation (Radio Shack)
EDS, a subsidiary of General Motors Trintex
Equifax
TRW
Source Telecomputing Corporation
Chase Manhattan Bank
Motorola
Ameritech
Bell Atlantic
Bell South
Southwestern Bell
NYNEX
Pacific Telesis
US West
Associated Credit Services, Inc.

Agency Views

U.S. Department of Justice,
Office of Legislative and Intergovernmental Affairs,
Washington, DC, June 6, 1986.

Hon. Peter Rodino, Jr.,
Chairman, Committee on the Judiciary,
House of Representatives, Washington, DC.

Dear Mr. Chairman: This letter is to advise you of the Department of Justice's position with regard to H.R. 4952, the Electronic Communications Privacy Act of 1986, which we understand is scheduled for markup on June 10 by the full House Judiciary Committee. This bill makes important changes to the existing wiretap statutes and fills gaps in current laws by creating provisions to regulate interception of and access to new forms of electronic communication such as data transmissions.

The Department of Justice has worked intensively on this legislation over the past several weeks with the members and staff of the Subcommittee on Courts, Civil Liberties and the Administration of Justice, as well as with interested representatives of industry and civil liberties groups. While initial versions of this legislation did not in our view adequately safeguard legitimate and vital law enforcement and national security needs for access to communications, as a result of the negotiations that have occurred the bill has been substantially modified to accommodate our concerns. In our judgment the bill as presently drafted fairly balances the interests of privacy and law enforcement and its enactment would represent a major accomplishment of the 99th Congress, holding forth the promise of significant benefits for business, privacy, and law enforcement alike.

Accordingly, the Department of Justice strongly supports the enactment of H.R. 4952.

Sincerely,

John R. Bolton,
Assistant Attorney General.

Section-by-Section Analysis

Section 1 provides the short title for the bill, the Electronic Communications Privacy Act of 1986.

Title I—Interception of Communications and Related Matters

Section 101 contains five subsections. Subsection (a) contains the definitions, and amendments to definitions, used in this chapter and in the new chapter 121 of title 18.

Subsection (a)(1) contains three subparagraphs. Subsection (a)(1)(A) amends the definition of "wire communication" to include aural transfers. The term "aural transfer" is defined in section 2510 (18) of this title. The term "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and point of interception. Thus, the amended definition is intended to encompass existing telephone services.[30] Digitized voice communications are included to the extent that the communication originates with human voice. As a result of this change, a company whose activities affect interstate commerce and which installs its own private telephone or electronic communication system would have that system covered by the statute.

By amending the definition of "wire communication" in subsection (a)(1)(B) to include communications utilizing wires, cables, or other like connections within a switching office, the Committee intends that "wire communication" be construed to include communications made over cellular systems (as defined in 47 C.F.R. § 22.2),[31] regardless of whether the communications are between two cellular telephones or between a cellular telephone and a "landline" telephone.

Existing law, which prohibits interception of wire communications or oral communications, was enacted prior to the development of cellular telecommunications and does not provide adequate privacy protection to conversations transmitted over a cellular system. The Department of Justice has taken the position that, under existing law, communications between a mobile radio telephone and a landline telephone are wire communications, but that conversations between two radio telephones and not carried in whole or in part by regular telephone lines are neither wire communications nor oral communications. Inasmuch as all cellular communications (whether mobile-to-mobile or mobile-to-landline) must pass through a mobile telephone switching office, the Committee bill will remedy this inadequacy and provide explicit privacy protection to all communications utilizing cellular radio.

[30] The term "other like connection" as used in section 2510(1) includes fiber optic cable.
[31] *Cellular System.* A high capacity land mobile system in which assigned spectrum is divided into discrete channels which are assigned in groups to geographic cells covering a geographic service area. The discrete channels are capable of being reused in different cells within the service area.

In the event that the evolution of cellular technology permits the switching or transmission of mobile-to-mobile service (or mobile-to-landline service) without the use of wire, cable, or other like connection, the Committee intends that cellular communications be included within the term "electronic communication". Because cellular communication is transmitted over a communication system currently regarded by the FCC as a common carrier,[32] the Committee also intends that such communication not be considered "readily accessible to the general public" at any time subsequent to the date of enactment, regardless of how a provider of cellular service is denominated by any state or how the FCC may classify any such provider in the future.

The Committee's intention of providing privacy protection to cellular communications in any event is also reflected in the specific inclusion in the legislation of penalties for the interception of such communications.[33]

Part of the impetus to clarify the illegality of interception of cellular communications has been provided by the advertisement of scanning receivers (popularly known as "scanners") specifically promoting eavesdropping on conversations transmitted over cellular systems. Apparently after the FCC allocated frequencies to cellular radio some manufacturers of scanners added the capability to stop at and receive signals transmitted on these frequencies. The Committee finds this development troubling, and expects that the future design and manufacture of scanners will take into account the privacy protections accorded cellular telephony in this legislation.

Section 101(a)(1) amends the definition of "wire communication" to include "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection * * * furnished or operated by any person engaged in providing or operating such facilities for the transmission of * * * communications affecting interstate or foreign commerce * * *." Similarly, section 101(a)(5) defines a new term "electronic communication" to include "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a * * * system that affects interstate or foreign commerce * * *."

By the inclusion of the element "affecting (affects) interstate or foreign commerce" in these provisions the Committee does not intend that the Act regulate activities conducted outside the territorial United States. Thus, insofar as the Act regulates the "interception" of communications, for example, it, like the Omnibus Crime Control and Safe Streets Act of 1968, regulates only those "interceptions" conducted within the territorial United States. *See Stowe* v. *Devoy*, 588 F.2d 336 (2d Cir. 1978), *cert. denied*, 442 U.S. 931 (1979), and cases cited therein. *See also Berlin Democratic Club* v. *Rumsfield*, 410 F.Supp. 144, 157 (D.D.C. 1976), *United States* v. *Toscanino*, 500 F.2d 267, 279–280 (2d Cir. 1974); *United States* v. *Cotroni*, 527 F.2d 708 (2d Cir. 1975). Similarly, the controls in section 201 of the Act regarding access to stored wire and electronic com-

[32] *See* Cellular Communications Systems, 86 FCC 2d 469, 496 (1981).
[33] *See* 18 U.S.C. § 2511(4)(b), as added by § 101(d)(2) of H.R. 4952.

munications are intended to apply only to access within the territorial United States.

Subsection (a)(1)(C) amends the definition of wire communication to delete the "common carrier" requirement. In the current environment, numerous entities provide electronic communications services beyond the traditional common carrier. Therefore, the Committee chose to extend federal jurisdiction to the maximum permissible constitutional limits by providing coverage of a person who provides or operates facilities for communications that affect interstate or foreign commerce. *See Heart of Atlanta Motel* v. *United States*, 379 U.S. 241, 258–259 (1964).

In the present telecommunications environment, a terminating or originating customer or subscriber will often have installed his own facilities to switch or otherwise process his incoming or outgoing traffic. One example of such equipment is the "private branch exchange", or PBX, typically owned or leased by the customer and located on his premises, and used to interconnect the customer's telephones and data terminals with one another and with the lines of the local exchange carrier, one or more interexchange carriers, and possibly other service providers. To the extent that electronic and wire communications passing through PBXs and other such equipment affect interstate commerce, the Committee intends that those communications be protected under Section 2511. The interception of an electronic or wire communication at a point on the customer's premises is thus as much a violation of Section 2511 as if the interception were made through the equipment of a communications carrier. Similarly, where a user has interconnected its own equipment into a private network, communications carried on the network are fully entitled to the protections of Section 2511.

Subsection (a)(1)(D) amends the definition of wire communication to exclude the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit.

By "cordless telephone" we refer *not* to a cellular telephone, but to the type of telephone which uses a short range (a few hundred feet) radio link between the handset and the base unit in place of the usual wire. Such telephones are regulated under Part 15, subpart E of the rules of the Federal Communications Commission (FCC), and are not licensed. Because the communications made on some cordless telephones can easily be intercepted with readily available technologies (such as AM radio), it would be inappropriate to make such interception a criminal offense. The absence of privacy protection has been noted by the FCC. 47 C.F.R. § 15.236(a) (requiring a label stating "PRIVACY OF COMMUNICATIONS MAY NOT BE ENSURED WHEN USING THIS PHONE"). This view also comports with some recent cases. *See* discussion of current law, *supra*. It should be noted that it is only the *radio portion* of the communication that is excluded. The wire portion of the communication remains fully covered in the same sense as a traditional wire telephone conversation.

Subsection (a)(2) amends the definition of oral communication to exclude electronic communications. An oral communication is an utterance by a person under circumstances exhibiting an expectation that the communication is not subject to interception, under

H. Rept. 99-647 2

circumstances justifying such an expectation. In essence, an oral communication is one carried by sound waves, rather than by an electronic medium.

The definitions of wire communication and oral communication are not mutually exclusive. Accordingly, different aspects of the same communication might be differently characterized. For example, a person who overhears one end of a telephone conversation by listening in on the oral utterances of one of the parties is intercepting an oral communication. If the eavesdropper instead taps into the telephone wire, he is intercepting a wire communication. There have been cases involving radio communications in which the court having determined that the radio communication was not a wire communication then analyzes it in privacy terms to determine if it is an oral communication. The Committee views this as an inappropriate consideration and the amendment to 18 U.S.C. 2510(2) rejects that case analysis. *See, e.g., United States v. Rose*, 669 F.2d 23 (1st Cir. 1982).

Subsection (a)(3) amends section 2510(4) of title 18 to provide a definition for the term "intercept" with respect to electronic communications. The definition under current law of "intercept" is retained with respect to "wire" and "oral communications" with one exception. The Committee added the term "or other" after "aural". This change is intended to make clear that it is illegal to intercept the non-voice portion of a wire communication such as the data or digitized portion of a voice communication. The term intercept with respect to "electronic communications" is defined to mean "the interception of the contents of that communication through the use of any electronic, mechanical or other device".

Subsection (a)(4) amends section 2510(8) to strike the words "identity of the parties to such communication or the existence". This amendment avoids any ambiguity about the legality of the use of "pen registers". The Supreme Court has clearly indicated that the use of pen registers does not violate either this chapter or the Fourth Amendment. This amendment makes that policy clear. In addition, this amendment should be read in conjunction with the new chapter on pen registers, chapter 206 of title 18. It does not, however, affect the installation on use of pen registers under the Foreign Intelligence Surveillance Act. 50 U.S.C. 1801 *et. seq.* This amendment also makes clear the distinction between contents of communications and transactional records. The omission of a conforming amendment to the definition of "contents" in section 705 of title 47 is not intended to affect the current law under that section with respect to pen registers. The use of pen registers has been found not to violate section 705. *See Hodge v. Mountains Tel. & Telegraph Co.*, 555 F.2d 254 (19th Cir. 1977).

Subsection (a)(5) adds six new definitions to the chapter. Section 2510 is amended by adding a new subsection (12) to define "electronic communications". This expansion permits the inclusion in the general wiretapping and bugging law of many new forms of communication. For example, digitized transmissions and electronic mail will be provided with protection against interception. The definition of electronic communication means "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electro-

magnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include any wire or oral communication." Excluded from the definition of "electronic communication" are: (1) the radio portion of a cordless telephone communication; (2) any wire or oral communication; (3) any communication by a tone-only paging device; or (4) any communication from a tracking device.

The term "electronic communication" is intended to cover a broad range of communication activities that affect interstate or foreign commerce, except that the term does not include either oral or wire communications. As a rule, a communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterized as one containing the human voice (carried in part by wire). Communications consisting solely of data, for example, and all communications transmitted only by radio would be electronic communications.

A wire communication encompasses the whole of a voice telephone transmission even if part of the transmission is carried by fibre-optic cable or by radio—as in the case of cellular telephones and long-distance satellite or microwave facilities. This result is generally in accord with the case law. *See United States v. Clegg*, 509 F.2d 605, 611 (5th Cir. 1975); *United States v. Gregg*, 629 F. Supp. 958, 963 (W.D. Mo. 1986). Moreover, the conversion of a voice signal to digital form for purposes of transmission does not, in itself, render the communication non-wire; the provider's choice of transmission technology should not be dispositive. The Committee has intentionally omitted from the definitions any indication that a wire communication cannot also exhibit some of the characteristics of an electronic communication.

It should be noted that an improperly mechanical reading of the phrase "in whole or in part * * * by the aid of wire * * *" could sweep in virtually all voice communications made with the aid of any electronic equipment, inasmuch as virtually all such equipment includes in its assembly some length of wire or the equivalent. The Committee, however, intends the quoted phrase to refer to wire that carries the communication to a significant extent from the point of origin to the point of receipt, and not to wire that is found inside the terminal equipment at either end of the communication. On the other hand, communications over a length of wire that connects two telephones in the same building would be protected as wire communications. Similarly a cellular telephone system which uses either the wire-line system or wires in a switching station is covered as a wire communication.

A transaction may consist, in parts, of both electronic communications and wire or oral communications. For example, the transmission of data over the telephone is an electronic communication, but if the parties used the line to speak with one another between data transmissions, they would then be making a wire communication. And, indeed, a party's utterances into the telephone mouthpiece are an oral communication. The rules governing interception or disclosure may be different for each type of communication. The Committee understands that the Department of Justice will apply for a court order under the "wire" standards in cases where a tap may intercept mixed wire and electronic communications. As long

as the wire standards are followed a single court order should suffice to authorize the interception of both wire and electronic communications involving the same lines or instruments.

Inclusion of the term "radio" in the definition of "electronic communication" in Section 2510(12) reflects the fact that radio communications come within the scope of chapter 119. A number of other provisions, however, affect the legality of the interception of radio communications under chapter 119. The Committee does not intend any of the provisions directed specifically to radio to affect the applicability of Section 705 of the Communications Act of 1934, as amended, to actions by members of the public.

Subsection (a)(5) also adds a definition for the term "user." "User" means any person or entity who uses an electronic communication service and is duly authorized by the provider of such service to engage in such use.

Interception of closed circuit television communications is only included in the bill in a limited fashion. If a person or entity transmits a closed circuit television picture of a meeting using wires, microwaves or other method of transmission, the transmission itself would be an electronic communication and interception of the picture at any point without either consent or a court order would be in violation of the statute. By contrast, if law enforcement officials were to install their own cameras and create their own closed circuit television picture of a meeting, the capture of the video images would not be an interception under the statute because there would be no interception of the contents of an electronic communication. This would be so even if the law enforcement agency utilized the wiring in the premises to insall the cameras and transmit the images. Intercepting the audio portion of the meeting would of course be an interception of an oral communication and the statute would apply to that portion.

Under the Fourth Amendment and recent case law in the area, law enforcement authorities are bound to seek a court order based on probable cause to place a closed circuit television camera in premises where there is a reasonable expectation of privacy without at least one party consent. The whole area of closed circuit television is suitable for Congressional action and is a likely subject of legislation in the future. *See* H.R. 3456 (Kastenmeier) (applying Title III standards to video surveillance) The Committee is aware that the Department of Justice follows the rules established by the leading cases in this area in seeking closed circuit television orders,** and the Committee believes this is a wise procedure pending either legislation on the subject or a final judicial resolution of these issues.

Subsection (a)(5) also adds a new definition for "electronic communication system" to mean any wire, radio, electronic photoelectronic or photooptical facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

Subsection (a)(5) adds a definition for "electronic communication service" to mean any service which provides to users thereof the

** United States v. Torres, 751 F.2d 875 (7th Cir. 1984); see also *United States v. Biasucci*, 786 F.2d 504 (2d Cir. 1986).

ability to send or receive electronic communications or wire communications. These services can be provided through the same facilities. Common carriers like existing telephone companies are deemed providers of an electronic communication service.

Subsection (a)(5) adds a definition for the term "readily accessible to the general public." This term is used in section 2511(2) which creates an exception to the general prohibitions on interception. The new paragraph (16) states "readily accessible to the general public" means with respect to a radio communication, that such is not in one of five separate categories. In other words, if a radio communication fits into one of the five categories then it will have privacy protection (unless some other exception applies to preclude coverage). The first category of protected communications** is radio communications which are scrambled or encrypted. The terms scrambled or encrypted are used in their technical sense. To "Encrypt" or to "Scramble" means to convert plaintext into unintelligible form by means of equipment intended to protect the contents of a communication from unintended recipients. Equipment which merely changes the form of a plaintext message, e.g., a device which converts an analog signal to a digital stream, does not provide "encryption" within the meaning of this bill. The use of a word code, no matter how sophisticated, would not suffice. Examples of scrambling techniques which are currently available include the data encryption standard (DES).

The second type of protected communications is spread spectrum radio communications. These radio signals are transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication. *See* 50 FED. REG. 25234 (June 18, 1985). *Spread spectrum* technology usually involves the transmission of a signal on different frequencies and the receiving station must possess the necessary algorithm in order to reassemble the signal.

The third type of protected communications is radio communications carried on a subcarrier or other signal subsidiary. This category includes, for example, data and background music services carried on FM subcarriers and data carried on the vertical blanking interval (VBI) of a television signal. Under Section 2511(2)(g)(ii)(I), however, it is not unlawful to intercept subcarrier and VBI communications that are transmitted for the use of the general public, *e.g.*, the stereo subcarrier used in FM broadcasting, or data carried on the VBI to provide closed-captioning of television programming for the hearing-impaired.

The fourth type of protected communications is those which are carried by common carriers. There is an exception for tone-only paging systems. Thus, the interception of tone-only paging system transmissions will not be prohibited by this law. On the other hand, the unauthorized interception of a displaying paging signal intended for digital display by the paging receiver (which involves the transmission of alphanumeric characters over the radio) carried by a common carrier is illegal.

** Protected communication as used in this description means that the communication is otherwise legally protected against interception absent the applicability of some other exception such as one party consent.

The fifth type of protected communications consists of certain types of radio signals. Included in this category are satellite communications, auxiliary broadcast services and private microwave services. Each of these services routinely carries business or personal communications made with an expectation of privacy. These categories are described by reference to certain parts of the Rules of the Federal Communications Commission. This category excludes certain communications which are essentially two-way voice radio communications.

Part 25 of the FCC's Rules regulates communications made by satellite. Such communications are not defined to be readily accessible to the general public. Two other provisions of this Act, however, limit the liability incurred under chapter 119 by the interception of certain types of satellite communications. Section 2511(g)(iii)(II) exempts activities covered by section 705(b) of the Communications Act, relating to the interception or receipt of certain satellite cable programming for private viewing; accordingly, such activities are not unlawful under chapter 119. Section 2511(4)(b)(iii) further provides that it is not an offense under Section 2511(4) to intercept an unscrambled and unencrypted "network feed"—*i.e.*, a satellite transmission *that is transmitted to a* broadcasting station for purposes of retransmission to the general public—so long as the conduct is not for the purposes of direct or indirect commercial advantage or private financial gain.

Also excluded from the category of readily accessible radio communications are those transmitted on frequencies allocated under subparts D, E, and F of Part 74 of the FCC's Rules. Under the FCC's Rules, these frequencies may be licensed only to broadcasters. 47 C.F.R. §§ 74.432, 74.532, 74.632. Each of the subparts regulates communications that are entirely internal to a broadcast operation. They include, for example, video and audio transmissions from a news team in the field to the studio, and transmission from the studio to the transmitter site. Part 74 transmissions may also include two-way voice communications, such as those between studios and remote crews; but this Act provides an exception for such two-way voice communications made on frequencies shared with services outside Part 74. The interception of communications on such shared frequencies is not unlawful under chapter 119.

The final service excluded from the category of readily accessible radio communications is that regulated under Part 94 of the FCC's Rules, the private operational fixed microwave service. This service carries confidential business data. Under limited conditions, it may also be used to transmit certain types of television material. Transmissions under Part 94 are generally made with the intent of maintaining privacy, and it would be inappropriate to disrupt ongoing business practices by making those communications available to competitors and to other members of the public.

Subsection (a)(5) also provides a definition for "electronic storage". That term means "any temporary intermediate storage of a communication incidental to the electronic transmission thereof and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." Section 2510(17) defines "electronic storage" to mean any temporary, intermediate storage of a communication incidental to

the electronic transmission thereof, and any storage of such communication by an electronic communication service for purposes of backup protection of such communication. Under Section 2710, computer storage is defined as an element of "remote computing service". These definitions are not intended to limit the terms "electronic storage" or "computer storage" to any particular medium of storage. While storage often takes place within the random access memory of a computer, the term applies equally to storage in any other form, including that on magnetic tape, disks, or other media. Thus, for example, the prohibitions against unauthorized access to a wire or electronic communication while it is in electronic storage, as set forth in Section 2701, would prohibit unauthorized access to such a communication while it is stored on magnetic tape or disk. The prohibitions would apply similarly to information held on magnetic tape or disk pursuant to an agreement to provide remote computing service.

Subsection (a)(5) adds a new definition for the term "aural transfer". "Aural transfer" means a "transfer containing the human voice at any point between and including the point of origin and the point of reception". Under this definition voice messages transferred over a paging system are protected. It is intended that computer-generated or otherwise artificial voices are not included in this definition and thus will not be part of a "wire communication". They would, however, be part of an "electronic communication".

Subsection 101(b) makes three different types of amendments to existing title 18.

Subsection (b)(1) amends section 2511(2)(d) of title 18 by striking out "or for the purpose of committing any other injurious act". Under current federal law it is permissible for one party to consent to the interception and recording of a conversation. This exception to the general prohibition on interception, however, contains an exception relating to persons who intercept or record communications for illegal, tortious or other injurious purposes. This exception was added in 1968 by the late Senator Hart in an effort to prevent one party from intercepting or recording a conversation for blackmail or similar improper purposes. Unfortunately, that floor amendment was not drafted with precision. As a result, numerous court cases have arisen wherein the term "other injurious purposes" has been construed and misconstrued. Most troubling of these cases have been attempts by parties to chill the exercise of First Amendment rights through the use of civil remedies under this chapter. For example, in *Boddie* v. *American Broadcasting Co.*, 731 F.2d 333 (6th Cir. 1984), the plaintiff, whose conversations were recorded by a journalist, sued. Despite the consent of the reporter who was a party to the conversation, the plaintiff claimed that the recordation was illegal because it was done for an improper purpose (e.g., to embarrass the plaintiff). The court's opinion suggests that if the network intended to cause "insult and injury" to plaintiff Boddie, she might be entitled to recover. This interpretation of the statute places a stumbling block in the path of even the most scrupulous journalist. Many news stories have been brought to light by recording a conversation with the consent of only one of the parties involved—often the journalist himself. Unfortunately, many news

stories are embarrassing to someone. The present form of the statute not only provides such a person with a right to bring suit, but it also makes the actions of the journalist potentially a criminal offense under section 2511, even if the interception was made for the purpose of committing neither a criminal act nor a tort. The statute thus presents the journalist with a hard choice: to get the news may expose him or her to a criminal conviction and/or civil liability. And whether a journalist is convicted in fact may turn, under *Boddie*, on how a jury sitting years later assesses the journalist's subjective intent. The Committee finds such a threat to be inconsistent with the guarantees of the First Amendment. Inasmuch as the amended statute continues to prohibit interceptions made for the purpose of committing either a crime or a tort (including acts of defamation), the Committee believes that the public will be afforded ample protection against improper or unscrupulous interception. The amendment is intended to remove only the shadow of a finding that section 2511 has been violated by interceptions made in the course of otherwise responsible news gathering. While the appeals court decision merely sent the case back for further factual development, it is clear from the facts of the case that the term "improper purpose" is overly broad and vague. The deletion of the term leaves in place the exception to one party consent for illegal or tortious interceptions or recordation. Thus, the original purpose of the Hart amendment is preserved without maintenance of the litigation-breeding phrase. This amendment is supported by the Department of Justice.

Subsection (b)(2) amends section 2511(2)(f) to expand the exception applicable to foreign intelligence activities to make sure the provisions of chapter 121 do not adversely affect such activities.

Section 101(b)(2) of H.R. 4952 amends section 2511(2)(f) of Title 18 to ensure that nothing in chapter 119 or chapter 121 of Title 18 as amended by H.R. 4952, *affects existing legal authority for* United States Government foreign intelligence activities involving foreign electronic communications systems. The provision neither enhances nor diminishes existing authority for such activities; it simply preserves the status quo. It does not provide authority for the conduct of any intelligence activity.

Further the Committee expects that the practice of providing to the House and Senate Intelligence Committees proposed changes in relevant executive branch procedures and regulations governing the conduct of intelligence activities, including those involving electronic surveillance, physical searches, and the minimization of information collected concerning U.S. persons will be continued. As in the past, the Committee expects that any relevant changes in these procedures and regulations will be provided to the intelligence committees prior to their taking effect.

Finally, as has been noted before, since Congress last addressed the issue of privacy of communications in a comprehensive fashion, the technologies of communication and interception have changed dramatically, and are expected to continue to do so. These factors have raised serious issues about the protection of the privacy interests of U.S. citizens, which are of great concern to this Committee and to the American people. For this reason, the Committee wishes to emphasize the obligation of the heads of intelligence agencies to

continue to keep the Permanent Select Committee on Intelligence fully and currently informed of all intelligence activities pursuant to Title V of the National Security Act of 1947.

Section 107 of H.R. 4952 emphasizes that nothing in Title I of the bill or the amendments made by Title I, such as the changes made to 18 U.S.C. 2511(2)(f), provides authority for the conduct of any intelligence activity.

Subsection (b)(4) of section 101 of the bill amends section 2511(2) to provide new exemptions from criminal liability which are appropriate to the new types of technologies which are added to the privacy protection of the federal wiretap law. Thus, the bill lists a series of types of interceptions which are permissible.

The Committee has drafted the present Act with an eye to its interplay with Section 705(a) of the Communications Act of 1934. In particular, where this bill provides that "it shall not be unlawful" for the public to engage in specific conduct with respect to radio transmissions, the Committee intends that such a provision does not "authorize" the conduct for purposes of the first sentence of Section 705(a) of the Communications Act. Accordingly, the legality of such conduct remains subject to inquiry under the Communications Act. In contrast, where the bill provides that a specified person "may" engage in certain conduct, or uses similar language in the affirmative, the Committee intends that such a provision does "authorize" the conduct for purposes of Section 705(a). The legality of such conduct would be determined under Title 18. In addition, where judicial interpretations have previously determined that certain types of activities are implicitly authorized for purposes of Section 705, that interpretation is intended to continue in effect. *See, e.g., United States* v. *Freeman*, 524 F.2d 337, 340 (7th Cir. 1975), *cert. denied*, 424 U.S. 920 (1976).

The first exemption is a generic exception. It is permissible to intercept electronic communications made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public. The term "configure" is intended to establish an objective standard of design configuration to begin determining whether a system receives privacy protection. An example of systems which are readily accessible include loud speakers hooked up to a telephone system.

It should be noted that the term "readily accessible to the general public" is a defined term with respect to radio communications. See discussion, at ——, *supra*. Under section 101(b)(4) nothing carried by wire is "readily accessible to the general public".

Nothing in the bill affects the use of radar detectors, because the radar transmissions are readily accessible to the general public. Nothing in the bill, however, affects the authority of states to regulate the use of radar detectors.

The second set of exceptions relate to specific types of radio communications which have traditionally been free from prohibitions on mere interception. Thus, it is permissible to intercept any radio communication which is transmitted (1) by any station for the use of the general public,[44] or that relate to ships, aircraft, vehicles or persons in distress; (2) by any governmental, law enforcement, civil defense, or public safety communications system, including police and fire, readily accessible to the general public; (3) by a station operating on a frequency assigned to amateur, citizens band or general mobile radio services, or (4) by any marine or aeronautical communications system.

Amateur radio communications, including those utilizing telephone interconnect or amateur radio computer linked message systems, are certainly not those to which this legislation is aimed. *All* amateur radio communications conducted on radio frequencies allocated to the Amateur Radio Service *are* exempt from the electronic communications intercept prohibitions of the bill.

It *should* be noted that amateurs, in performing their public service functions, occasionally utilize communications of other services, such as NOAA weather broadcasts and the like. As such, many amateurs employ "scanner" receivers which are capable of receiving communications of many different radio services (including amateur VHF and UHF communications, typically). The use of, as an example, a multiband radio receiver by a licensed amateur should not subject the amateur to criminal prosecution or harassment in any fashion. Amateurs have legitimate reason to monitor frequencies outside the amateur bands. Many amateurs, for instance, are enrolled in the Military Affiliate Radio System and the Civil Air Patrol, which use frequencies assigned to the Department of Defense. Others are members of the Coast Guard Auxiliary using frequencies in the Maritime Service allocation. Some 30,000 amateurs are part of Skywarn, a system operated by the National Weather Service for tracking and warning of severe weather conditions, e.g., tornadoes; at times it may be required that they monitor Government frequencies in connection with this work. In short, there is legitimate reason for amateurs to have equipment which tunes beyond amateur bands.

The Committee considered listing all the existing radio services which are exempt from the bar on interceptions, but rejected that approach because it would have been cumbersome, possibly redundant, and would have had a built-in obsolescence. When the Committee asked the Federal Communications Commission for a list of radio services which were currently regulated by the FCC of the same kind as those listed in the bill, they provided a list of more than 40 such services. Such a list is extremely lengthy and the nomenclature used is frequently changing. Therefore, instead of listing all of these services the Committee listed some of the more common radio services. In addition, the bill includes a "generic" exception relating to radio services which are "readily accessible to the general public." Thus, for example, private land mobile services (currently licensed under Part 90 of the FCC Rules) are exempt from the prohibition on interceptions.

This subsection also exempts from coverage any conduct which is also prohibited by section 633 of the Communications Act of 1934.

[44] These include all communications transmitted for the use of the general public, including audio and television broadcast signals transmitted under Part 73 of the FCC Rules.

Thus, if an individual violates the criminal prohibitions in section 633 (relating to cable piracy) they cannot also be charged under this chapter of title 18.

The subsection also exempts conduct which is excepted from section 705(a) of the Communications Act by virtue of section 705(b) of that Act. Thus, if conduct is permitted under section 705(b) it would not be a crime under this chapter of title 18. Determination of whether conduct is permitted under section 705(b) must, of course, be the result of an examination of the statute, relevant legislative history, existing court interpretations, and constructions given the statute by appropriate federal regulatory entities.

With respect to the interception of radio communications by home satellite dishes, the Committee does not intend to make criminal any type of conduct that is currently lawful under Section 705 of the Communications Act and the present Wiretap Act. To remove any doubts about its impact on home satellite dish owners, H.R. 4952 contains a provision expressly stating that it is not unlawful under Title 18 to intercept unscrambled network programming feeds to affiliates—*i.e.*, communications "transmitted to a broadcasting station for purposes of retransmission to the general public"—unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain. Accordingly H.R. 4952 does not create a new class of criminal conduct concerning interception of radio communications by home satellite dishes. In order to violate Title 18, moreover, an interception must be "willful". Incidental or inadvertent interception of a protected video signal which does not benefit a home dish owner would not constitute a criminal violation of the statute. H.R. 4952, in short, is carefully drafted to remain as neutral as possible with respect to the coverage of both Section 705 and Title 18 as to interception of radio signals by home satellite dish owners. "Private gain" is a term defined in section 705(b) and the meaning given there is intended to apply to this section as well.

H.R. 4952 adds a new Section 2511(4)(c) which exempts from Title 18 the reception by home earth station owners of certain unscrambled satellite transmissions, as long as such reception is not for commercial advantage or private gain (including any use by a commercial establishment). While the bill does not make criminal any type of conduct with respect to interception of radio communications by home satellite dishes that is currently lawful under section 705 of the Communications Act and the provisions of Chapter 119 of Title 18, the specific exemption in this subsection does not apply to the interception of private communications via satellite such as sporting events when they are not the final output of a national television network to a broadcasting station for purposes of retransmission to the general public.

However, even the unscrambled satellite transmission which is not protected under Title 18 because it comes within Section 2511(4)(b)(iii) may in fact be a private communication, and H.R. 4952 is not intended to exempt such noncommercial interception from liability, if any, under Section 705 of Title 47 or otherwise "authorize" interception of unscrambled transmissions for noncommercial purposes. Rather, the intention of the Committee is that the legality of noncommercial interception of this type of unscram-

bled satellite transmission will be decided under Section 705 of the Communications Act. The Committee expresses no view on this issue. The Committee notes, however, that it is the view of the General Counsel of the FCC that interception and viewing by home earth station owners of television network satellite feeds to local affiliated television stations could subject the interceptor to civil and criminal penalties under the Communications Act. *See*, Letter of Jack D. Smith to Honorable Robert Kastenmeier, Chairman, Subcommittee on Courts, Civil Liberties and the Administration of Justice, November 27, 1985. *Compare National Football League* v. *McBee & Bruno's*, — F.2d— (8th Cir. June 4, 1986) (individual interception of "clean feeds" not permanently enjoined because of equitable considerations).

[The letter follows:]

FEDERAL COMMUNICATIONS COMMISSION,
Washington, DC, November 27, 1985.

Hon. ROBERT W. KASTENMEIER,
Chairman, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, Washington, DC.

DEAR CONGRESSMAN KASTENMEIER: At a recent meeting between congressional and Commission staff, David Beier requested that my office issue an opinion on the applicability of Section 705 of the Communications Act to network television feeds. Specifically, we were asked whether Section 705 prohibits owners of satellite antennas from intercepting the networks' television feeds as they are being distributed to their affiliates via satellite. In general, those transmissions contain network programming and the national commercial spots. Local advertising and programming are added at the affiliates' broadcast station. Thus, by intercepting the networks' satellite feeds, viewers are seeing essentially the same programs as other television viewers but without certain commercials.

Section 705 provides, in pertinent part that

> No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. . . . This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by any station for the use of the general public.

The courts, in several civil and criminal actions, have been the primary interpreters of Section 705. Unfortunately, none of the decided cases are directly on point in that they do not apply to the interception of satellite network feeds. However, the case law applying Section 705 to MDS transmissions strongly suggests that Section 705(a) prohibits the unauthorized interception of satellite network feeds.

The networks' satellite feeds clearly constitute interstate radio communications. Viewing those transmissions constitutes a use by the owner of the satellite antenna of the signal "for his own benefit". *See e.g., Movie Systems, Inc.* v. *Heller*, 710 F. 2d 492 (8th Cir. 1983); *Hoosier Home Theater, Inc.* v. *Adkins*, 595 F. Supp. 389 (S.D.

Ind. 1984). The networks and their local affiliates fund their operations from advertising revenues, which, in turn, are a function of the size of the viewing audience. Because some local commercials are not carried on the network feeds, owners of satellite antennas would not see those commercials and hence would not generally be counted as part of the viewing audience. Therefore, unauthorized interception of the satellite network feeds has the effect of reducing the networks' audience and, as a consequence, their affiliates' operating revenues. In economic terms, this appears to be analogous to the unauthorized interception of subscription television signals without payment.

Section 705(a) expressly excludes from its prohibition radio communications transmitted for the use of the general public. Satellite transmissions, like MDS transmissions, are, however, a common carrier service provided on common carrier frequencies. *See Movie Systems, Inc.* v. *Heller, supra* at 495; *Home Box Office, Inc.* v. *Advanced Consumer Technology, Movie Antenna, Inc.*, 549 F. Supp 14, 24 (S.D.N.Y. 1981); *Chartwell Communications Group* v. *Westbrook*, 637 F.2d 459, 465 (6th Cir. 1980). For the reason discussed above concerning advertising revenues, they are not intended to be viewed by the general public in the form they are transmitted from satellites. Additionally, in determining the applicability of this exclusion, the critical factor is the intent of the party transmitting the radio communications. *See Chartwell Communications Group* v. *Westbrook, supra* at 464–465. The networks are of course the ultimate authority on their intent. It appears that network satellite feeds are only intended for reception by their affiliates. We believe that the networks are considering scrambling these transmissions in order to preclude their interception. Existing case precedent does not require, however, that networks scramble their signals in order to be encompassed within Section 705. *See Home Box Office, Inc.* v. *Advanced Consumer Technology, Movie Antenna, Inc., supra* at 21–22; *Hoosier Home Theater, Inc.* v. *Adkins, supra* at 396.

Finally, we recognize that under certain conditions, Section 705(b) further excepts from the prohibition of 705(a) the interception of satellite cable programming for private viewing. The satellite network feeds are not, however, satellite cable programming as that term is defined in Section 705(c)(1). Thus, Section 705(b) does not otherwise sanction the interception.

In summation, Section 705(a) appears to encompass the network satellite feeds. Unauthorized interception of those signals by home owners with satellite antennas or the unauthorized sale of decoders could lead to civil or criminal actions under Section 705. *See e.g., Movie Systems, Inc. v. Heller, supra; United States v. Westbrook*, 502 F. Supp. 588 (E.D. Mich. 1980).

Sincerely yours,

JACK D. SMITH, *General Counsel.*

Subsection (g)(iv) also exempts from the criminal prohibitions the interception of any electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of such interference. This exemption was suggested by the Association of North

American Radio Clubs (ANARC) and meets the needs of the Federal Communications Commission.

Finally, this subsection, (g)(v), exempts the interception of a radio communication which is made for other users of the same frequency when such communication is made through a common carrier system that utilizes frequencies monitored by individuals engaged in the provision or use of such a system, as long as the communication is not scrambled or encrypted. This exception will permit the monitoring of shared channels on marine radio which utilizes an onshore operator.

Subsection (b)(4) also amends section 2511(2) to add a new subsection (h). Proposed subsection (h)(i) clarifies that this chapter does not regulate the use of pen registers. The new subsection (h)(ii) states that no violation of this chapter occurs if a provider of wire or electronic communication service records the fact that a communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication or user of that service, from fraudulent, unlawful or abusive use of such a service. This provision permits the electronic and wire communication providers to protect themselves and their customers. Thus, the Committee continues the current law and practice with respect to activities of telephone companies to protect themselves against fraud, abuse or unlawful use. *See United States* v. *Auler*, 539 F.2d 642 (7th Cir. 1976), *cert. denied*, 429 U.S. 1104 (1977); *United States* v. *Goldstein*, 532 F.2d 1305 (9th Cir.), *cert. denied sub nom. Roberts* v. *United States*, 429 U.S. 960 (1976); *United States* v. *Freeman*, 524 F.2d 337 (7th Cir. 1975), *cert. denied*, 424 U.S. 920 (1976); *United States* v. *Clegg*, 509 F.2d 605 (5th Cir. 1975); *United States* v. *Shah*, 371 F. Supp. 1170 (W.D.Pa. 1974).

Proposed subsection (h)(iii) states that it is not unlawful to use a "trap and trace" device. *See Michigan Bell Tel. Co.* v. *United States*, 565 F.2d 385 (6th Cir. 1977) (upholding the use of trap and trace devices under Federal Rule of Criminal Procedure. Rule 41)

Subsection (c) provides technical and conforming amendments. Subsection (c)(1) adds "electronic communication" in appropriate places throughout the chapter.[97] Subsection (c)(2) amends the heading of the chapter. Subsection (c)(3) amends the table of chapters to add electronic communications to the table. Subsection (c) (4), (5), (6) and (7) makes appropriate technical amendments to delete the term "common carrier" and substitute in its place "provider of wire or electronic communication service."

Section 2511(2)(a)(i), as amended, specifies that it is not unlawful for the employees of providers of wire or electronic communication services to intercept customer communications in the normal course of employment while engaged in any activity which is a nec-

[97] Similarly it should be noted that the amendments to section 2511(2)(d) (relating to one-party consent) also apply to private microwave services. It is the Committee's intent to extend the exemption with respect to one—party consent in section 2511(2)(d) to electronic communications. For example, if a licensee of a private microwave system, licensed pursuant to Part 94 of the Federal Communications Commission's Rules, or the operator of a private [illegible] or private fiber optic system secures consent for the licensee's or operator's recording and/or monitoring of communications over that private system from one of the parties to the communication, such recording and/or monitoring is permissible.

essary incident to the rendition of the service or to the protection of the rights or property of the provider, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality checks. In applying the second clause only to wire communications, this provision reflects an important technical distinction between electronic communications and traditional voice telephone service. The provider of electronic communications services may have to monitor a stream of transmissions in order properly to route, terminate, and otherwise manage the individual messages it contains. These monitoring functions, which may be necessary to the provision of an electronic communication service, do not involve humans listening in on voice conversations. Accordingly, they are not prohibited. In contrast, the traditional limits on service "observing" and random "monitoring" do refer to human aural interception and are retained with respect to voice ("wire") communications.

Subsection (d) modifies the general penalty structure for criminal violations of this chapter. The general rule is that a willful violation is punishable as a five year felony. Thus, unless one of the exceptions applies to a person found guilty of willfully violating one of the criminal statutes in the chapter, they will be liable for a fine under the chapter[98] and imprisonment of up to five years or both.

The first exception for this general rule is that the interception of radio communications are punishable as one year misdemeanors, with fines of up to $100,000 18 U.S.C. 3623. There are three exceptions to this general rule. If the offender has been previously found to have been guilty of an offense of intercepting radio communications, then the felony provisions apply. Similarly, if the interception is done for illegal, tortious or commercial gain purposes, then the offender is punishable under the felony penalty. The second exception is that first offenders who intercept the radio portion of a cellular telephone call (and who act without one of the enumerated bad purposes) may only be subject to punishment of up to six months in prison or a $500 fine or both.

In the event that an offender intercepts the wire portion of a telephone call such conduct remains a five year felony.

The third exception is that conduct, otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of retransmission to the general public, is not an offense under this chapter and is not subject to civil liability, unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain. The terms "direct or indirect commercial advantage or private financial gain" are intended to have the same meaning as those terms have when used in 47 U.S.C. 705(b). This third exception decriminalizes the interception of "network feeds" under title 18. The exception does not extend beyond "network feeds." The

[98] 18 U.S.C. 3623 provides for a different maximum fine level for felonies, or misdemeanors resulting in death. Individual defendants can be fined up to [illegible] and organizations up to [illegible].

Committee notes that interception and disclosure or use may violate section 705 of the Communications Act. *See* note 9, *supra*.

The penalty structure assumes that more active participation is necessary when a person engages in traditional wiretapping or bugging; therefore, a higher degree of culpability attaches to such conduct. Similarly, higher penalties are justified for second or subsequent offenders or for offenders who engage in prohibited conduct for improper purposes. On the other hand the Committee recognized that although the criminal provisions of the chapter require "willful violations", interception of radio transmissions can be more easily achieved. Therefore, the Committee reduced the penalties for the interception of radio transmissions.

Subsection (e) amends section 2518(10) to provide that the remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions available for non-constitutional violations of this chapter involving such communciations. In the event that there is a violation of law of a constitutional magnitude the court involved in a subsequent criminal trial will apply the existing constitutional law with respect to the exclusionary rule. *Mapp* v. *Ohio*, 367 U.S. 643, 652 (1961); *Massachusetts* v. *Sheppard*, 104 S.Ct. 3424 (1984); *United States* v. *Leon*, 104 S.Ct. 3405 (1984).

Section 103 amends section 2511 of title 18 to add a new criminal prohibition on disclosure by adding a new subsection (3)(A). The new language provides that a person or entity providing wire or electronic communication service to the public shall not willfully divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or the agent of such addressee or intended recipient. The amendment to section 2511 made by § 102 includes the term "to the public" and hereby includes the government as part of the public. Thus, FTS services are included. The term "willfully" is used so as to conform this criminal prohibition with those in the rest of the chapter.

The term "willful" as used in this chapter has been construed—and misconstrued—by the courts. Note, An Analysis of the Term Willfull in Federal Criminal Statutes, 51 NOTRE DAME LAWYER 786 (1976). By retaining the same terminology the Committee does not intend to perpetuate the confusion which has emerged in the case law. See C. Fishman, *Wiretapping and Eavesdropping*, Cum. Suppl. 1986 section 7.15 pages 37–41. Thus, the Committee intends that the term have the same meaning as the term intentional. An "intentional" state of mind means that one's state of mind is intentional as to one's conduct or the result of one's conduct if such conduct or result is one's conscious objective. The intentional state of mind is applicable only to conduct and results. Since one has no control over the existence of circumstances, one cannot "intend" circumstances.

The term "intentional" is narrower than the dictionary definition of "intentional". "Intentional" means more than that one *voluntarily* engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective.

In contrast a knowing state of mind is (1) an awareness of the nature of the conduct, (2) an awareness of or a firm belief in the existence of the circumstance and (3) an awareness of or a firm belief in the substantial certainty of the result.

Thus, the distinction between an "intentional" state of mind and a "knowing" state of mind is narrow but important. As recently stated by Mr. Justice Rehnquist,

> Perhaps the most significant, and most esoteric, distinction drawn by [Model Penal Code] analysis is that between the mental states of "purpose" and "knowledge". As we pointed out in *United States* v. *United States Gypsum Co.*, 438 U.S 422, 445 (1978), a person who causes a particular result is said to act purposefully (intentionally) "when he consciously desires that result, whatever the likelihood of that result happening from his conduct"; while he is said to act knowingly if he is aware "that the result is practically certain to follow from his conduct, whatever his desire may be as to that result." [footnote omitted]
>
> In the case of most crimes, "the limited distinction between knowledge and purpose has not been considered important since 'there is good reason for imposing liability whether the defendant desired or merely knew of the practical certainty of the results.'" [citation omitted] * * *

In certain narrow classes of crimes, however, heightened culpability has been thought to merit special attention. *United States* v. *Bailey*, 444 U.S. 394 (1980).

The term "intentional" does not require that the act was committed for a particular purpose or motive. *See Senate Report* 97-307 at 67.

By the use of the term "willful" (throughout chapter 119)—and its accompanying definition—the Committee precludes the applicatin of civil or criminal liability for acts of inadvertent interception.

This section contains an exception to the limitations of divulgence. The exception applies to persons or entities providing wire or electronic communication service to the public. Such persons or entities are permitted to divulge the contents of any such communication if: (1) otherwise authorized in section 2511(2)(A) or 2517 of title 18; (2) with the consent of the originator of any addressee or intended recipient of such communication; (3) to any person employed or authorized, or whose facilities are used, to forward such communication to its destination, or (4) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime if such divulgence is made to a law enforcement agency.

The exceptions to the divulgence bar are relatively straightforward. Obviously providers should be permitted to divulge under other provisions of the chapter. To be consistent with the one party consent exception found in the chapter a similar exception is appropriate here. It is also logical to provide an exception with respect to activities necessary and intrinsic to the communication activity, therefore it is necessary to exempt communication intermediaries. Finally, if a communication provider inadvertently obtains the contents of a communication during transmission which appears to relate to the commission of a crime, divulgence is permitted when such divulgence is made to a law enforcement agency. If the provider purposefully sets out to monitor conversations to ascertain whether criminal activity has occurred this exception would not apply.

Section 103 amends—largely by recodifying—the existing section 2520 of title 18 to incorporate violations involving interception, disclosure or willful ** use of wire, oral or electronic communications. Proposed subsection (a) authorizes the commencement of a civil suit. The plaintiff may bring a civil action under Section 2520 whether or not the defendant has been subject to a criminal prosecution for the acts complained of; but in the absence of such prosecution and conviction, it is the plaintiff's burden to establish that the requirements of this section are met. Subsection (b) indicates that appropriate relief can include: (1) preliminary and other equitable or declaratory relief as may be appropriate; (2) damages and punitive damages; and (3) reasonable attorney's fees and other litigation costs reasonably incurred. Subsection (d) of proposed section 2520 provides a method for the computation of damages. *Under subsection (c) the court may assess damages consisting of whichever is greater of the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation or statutory damages of whichever is greater of $100 a day for each day of violation or $10,000.*

Subsection (d) provides a good faith defense to actions brought under this section. The term "good faith" as used in this section includes the receipt of a facially valid court order. Thus, the fact that the provider of electronic communication service also has received such a court order, means the provider would be entitled to a dismissal of a civil course of action upon a showing that such provider acted within the scope of the court order.

Subsection (e) of proposed section 2520 provides a statute of limitations for actions brought under this section. The subsection provides that any action may not be commenced later than two years after the date upon which the claimant first has reasonable opportunity to discover the violation.

Section 104 amends the list of federal officials who may make applications for court orders under this chapter. Section 2516(1) is amended to add to the list of officials who may be specifically designated by the Attorney General to authorize applications to include any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division. The addition of an acting Assistant Attorney General is not meant to imply rejection in any other context of the well-established principle that an acting official ordinarily possesses all the legal powers of the official for whom he is acting, *see Keyser v. Hitz*, 133 H.S. 138 (1890), but rather to clarify the law under this statute in light of its unique history and interpretation. *Compare, e.g., United States v. Acon*, 513

** The term "willful" is intended to have the same meaning as it does when used in other sections of this chapter.

F.2d 513 (3d Cir. 1975), with *United States v. Pellicci*, 504 F.2d 1106 (1st Cir. 1974), *cert. denied*, 413 U.S. 1122.

Section 105 amends section 2516(1) by adding new crimes which can be used to justify an application for wiretapping or bugging order. The new crimes include violation of the following title 18 provisions: (1) section 751 (relating to escape); (2) sections 2312 and 2313 (relating to automobile theft); (3) the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts); (4) section 1203 (relating to fraud and related activities in connection with access devices); (5) felony violations of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain interception devices); (6) section 3146 (relating to penalty for failure to appear); (7) section 3521 (relating to violations of the security of protecting witnesses); (8) section 32 (relating to destruction of aircraft or aircraft facilities); (9) section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire); (10) section 1952B (relating to violent crimes in aid of racketeering activity); (11) section 115 (relating to threats against a federal official); (12) the section in chapter 65 relating to destruction of an energy facility; (13) section 1341 (relating to mail fraud); and (14) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain intercepting devices). In addition, this section authorizes the application for orders under this chapter for the location of a fugitive from an offense described in this section.

Section 106(b) amends section 2516 to authorize the government to apply for a court order authorizing or approving the interception of an electronic communication by an investigative or law enforcement officer when an interception may provide evidence of a federal felony. Thus, for non-wire, non-oral electronic communications, a different and less restrictive list of crimes can be used to justify an application for interception. Section 106(b) permits the government to make applications for the interception of electronic communications. The Committee has been informed by the Department of Justice that for the three years which follow the date of enactment of this legislation that this exercise of authority will only be made pursuant to the approval of the same level of officials as those involved in the approval of applications for wire intercepts. In addition to this voluntary regulatory limitation, the Department of Justice has committed themselves to submit to the relevant Congressional committees any proposed changes in these regulations at least 90 days in advance of any change.

Section 106 contains four subsections. Subsection (a) provides that a court can authorize an order within the court's jurisdiction and outside that jurisdiction but within the United States in the case of a mobile interception device authorized within such jurisdiction. In the usual case the court will authorize the installation of a device, the device will be installed within the court's jurisdiction and the suspect will then move outside the court's jurisdiction. Nothing in this section affects the current law with respect to the use of such devices outside the United States. In certain cases a device authorized for installation, for instance, in an automobile may be authorized in one district and the vehicle might be moved to another district prior to installation. The authorization will

permit installation in the district to which the vehicle has been moved.

Subsection (b) amends section 2518(4) by striking out "at reasonable rates" and inserting in lieu thereof "for reasonable expenses incurred in providing such facilities or assistance." This is designed to permit reimbursement to be available at an appropriate amount in light of the work required for a particular activity. While in the ordinary case a flat or general rate may be appropriate, this change will permit flexibility to permit reimbursement at a higher level in unusual cases.

Subsection (c) makes two changes in section 2518(5) of title 18. Subparagraph (1) provides a rule for when the 30 days to install a tap or bug begins to run. Under this rule the 30 day time period commences on the earlier of the day on which the officer first begins to conduct an interception or ten days after the order is entered. Under this rule if an officer took 9 days after the entry of the order to effectuate the tap and began to overhear conversations then the 30 day time period would start from on the 9th day.

Subparagraph (2) of subsection (c) of section 106 of the bill provides a special minimization rule. Under this rule when an intercepted communication is in a code or foreign language and an expert in that foreign language or code is not reasonably available during that interception period, minimization may be accomplished as soon as practicable after the interception. In this regard, it is contemplated that the translator or decoder will listen to the tapes of an interception and make available to the investigators the minimized portions preserving the rest for later possible court perusal.

Subparagraph (2) of subsection (c) of section 106 of the bill also provides that the monitoring of interceptions under this chapter may be conducted in whole or in part by Government personnel, or by individuals operating under contract with the Government, as long as such personnel are acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception. This change, which was sought by the Federal Bureau of Investigation, is designed to free field agents from the relatively routine activity of monitoring interceptions so that they can engage in other law enforcement activities.

Subsection (d) of section 106 amends 2518 of title 18 to provide new rules with respect to the specificity required in the descriptions of the place to be bugged or tapped. Under current law, the application and the order must indicate the "particular" facility or place in which the interception is to occur. The amendments establish two largely similar rules, the specificity with which the locale of an interception of "oral communications" and "wire communications" can occur.

With respect to "oral communications" a limited list of federal officials can apply for a special order seeking relief under this provision. The application must contain a full and complete statement as to why the ordinary specification requirements are not practical. The application must also identify the person committing the offense and whose communications are being intercepted. The judge in turn must find that the ordinary specification rules are not practical. Examples of situations where ordinary specification rules

would not be practical would be a suspect who moves from room to room in a hotel to avoid a bug and who sets up a meeting with another suspect for a beach or field. In that case, the order could indicate authority to follow the suspect and engage in the interception once the targeted conversation occurs.

The rule with respect to "wire communications" is somewhat similar. An application for relief from the ordinary specificity rules must be made by a limited list of federal officials. The application must show that the person committing the offense has a purpose to thwart interception by changing facilities. In these cases, the court must find that the applicant has shown that such a purpose has been evidenced by the suspect. An example of a situation which would meet this test would be an alleged terrorist who went from phone booth to phone booth numerous times to avoid interception. Alternatively, a person whose telephone calls were intercepted who said that they were planning on moving from phone to phone or to a pay phone, to avoid detection would have demonstrated that purpose.

Both with respect to "wire" and "dral" communications, where the federal government has been successful in obtaining this relaxed specificity order the government cannot commence the interception until the facilities or place from which the communication is to be commenced is ascertained by the person implementing the interception order. In other words the actual interception could not commence until the suspect commences or evidences an intention to commence a conversation. Thus, it would be improper to use this expanded specificity order to tap a series of telephones, intercept all conversation over such phones and then minimize the conversations collected as a result. This provision puts the burden on the investigatory agency to ascertain when the interception to take place.

Section 107 subsection (a) provides that "* * * (n)othing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity. This provision clarifies that the amendments made in section 102(b)(3) are not read as constituting any new authority; rather those amendments represent an exemption from this chapter and chapter 121 for otherwise lawful activities.

Section 107(b)(1) exempts communications security monitoring from coverage by Chapter 119 or 121 of Title 18, United States Code. Communications security measures are protective measures taken to deny unauthorized persons information derived from United States Government telecommunications and to ensure the authenticity of such communications. Communications security protection results from the application of security measures to electrical systems generating, handling, processing, or using information the loss of which could adversely affect the national interest. Communications security monitoring is the systematic examination of telecommunications carried out to determine the adequacy of communications security deficiencies, to provide data from which to predict the effectiveness of proposed communications security measures, and to confirm the adequacy of such measures after implementation. Communications security monitoring is an essential part of such examinations and is conducted pursuant to detailed guidelines approved by the Attorney General. *Supra*, note 11. These procedures generally set forth an elaborate procedure to assure the communications security monitoring of private communications (as defined in para. 4.e.) is based on consent. *See* para. 5.b. and 6.a. of NASCI, 4000A. Communications security monitoring is the act of listening to, copying, or recording transmissions of the Executive Branch official telecommunications, including the communications of certain contractors, to provide technical material for analysis in order to determine the degree of security being provided to these transmissions. This security, includes, for example, that provided by cryptographic equipment. For purposes of communications security monitoring, government telecommunications are telecommunications of any employee, officer, contractor, or other entity of the United States Government which concern an official purpose of government and which are transmitted over a telecommunications system owned or leased by the United States Government or a Government contractor.

Subsection (b) of section 107 provides that this Act does not affect the conduct by officers and employees of the United States Government when such conduct is in accordance with other applicable federal law and if conducted in accordance with procedures approved by the Attorney General. *See e.g.*, Letter from William French Smith, Attorney General, to Lincoln D. Faurer, Director, National Security Agency, dated January 9, 1984 (relating to Guidelines For the Conduct of *Communications Security Monitoring Activities*, NACSI No. 4000A). The type of activity referred to in this proviso relates to one or more of three categories of activities: (1) interception of encrypted or scrambled or other official communications for communications security of United States Executive Branch departments or entities or United States government contractors **; (2) interception of radio communications transmitted between or among foreign powers or agents of foreign powers; or (3) accessing electronic communication systems used exclusively by a foreign power or an agent of a foreign power.

[The letter follows:]

OFFICE OF THE ATTORNEY GENERAL,
Washington, DC, January 9, 1984.

LINCOLN D. FAURER,
Lieutenant General, USAF,
Director, National Security Agency,
Ft. George G. Meade, MD.

DEAR DIRECTOR FAURER: The attached procedures governing the communications security (COMSEC) activities of the United States government meet the requirements of Executive Order 12333 and are otherwise lawful. Accordingly, they are hereby approved.

** Government contractor means an individual, corporation, partnership or other entity performing work under a United States Government contract.

[Paragraph regarding internal policy discussions unrelated to lawfulness of the procedures deleted.]

Sincerely,

WILLIAM FRENCH SMITH,
Attorney General.

Attachments.

NACSI NO. 4000

GUIDELINES FOR THE CONDUCT OF COMMUNICATIONS SECURITY MONITORING ACTIVITIES

1. REFERENCES

a. Communications Act of 1934, Public Law 73-416 (as amended).
b. Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351 (as amended).
c. Foreign Intelligence Surveillance Act of 1978, Public Law 95-511.
d. National Communications Security Directive, dated 20 June 1979.
e. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981.

2. INTRODUCTION

The basic purpose of communications security (COMSEC) monitoring is to provide unique material, not readily available through other sources, to evaluate the status of U.S. COMSEC. The information collected through the COMSEC monitoring program is similar to the information potentially available to foreign powers through their own signals intelligence (SIGINT) collection. Hypothetical projections of the vulnerability of telecommunications, procedures, equipment, and systems, based on technical analysis and modeling, do not always provide a comprehensive data base for analysis. COMSEC monitoring is, therefore, used to provide the empirical data necessary to conduct comprehensive analyses of these vulnerabilities and afford a basis for correcting them.

3. PURPOSE AND SCOPE

a. This Instruction provides policy and guidance for the establishment of COMSEC monitoring procedures consistent with applicable law and regulations.* It implements that portion of the National Communications Security Directive (Reference d.) which assigns the Director, National Security Agency (NSA), responsibility to issue guidelines for the conduct of COMSEC monitoring.

b. This Instruction is applicable to all Federal Government departments and agencies engaged in or using the results of COMSEC monitoring. It has been approved by the Attorney General.

* Although there are no Federal statutes specifically addressing COMSEC, References a., b., and c. will have an impact upon any COMSEC monitoring guidelines and procedures.

c. Technical surveillance countermeasures, electronic sweeps, surveillance of non-communications emissions (e.g., radar), and TEMPEST testing are not within the scope of this Instruction.

4. DEFINITIONS

a. *COMSEC*. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emissions security) to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to COMSEC information or materials.

b. *COMSEC Monitoring*. The act of listening to, copying, or recording transmissions of one's own official telecommunications to provide material for analysis in order to determine the degree of security being provided to those transmissions.

c. *Contents*. When used with respect to a communication, it includes any information concerning the identity of the parties thereto, or the existence or meaning of that communication.

d. *Electronic Surveillance*. The acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

e. *Private Communication*. A communication in which the parties thereto, in the absence of their consent to be monitored for COMSEC purposes, have a reasonable expectation of privacy.

f. *Telecommunications*. The transmission, communication, or processing of information, including the preparation of such information therefor, by electrical, electromagnetic, electromechanical, or electro-optical means.

g. *Telecommunications System*. The devices used to transmit and/or receive communications or process telecommunications, including the preparation of information, therefor; the devices may be electrical, electromagnetic, electromechanical, or electro-optical.

h. *Government Telecommunications*. Telecommunications of any employee, officer, contractor, or other entity of the U.S. Government which concern an official purpose of Government and which are transmitted over a telecommunications system owned or leased by the U.S. Government or a Government contractor. (See Telecommunications and Telecommunications System, above.)

5. POLICY

a. The Government will conduct COMSEC monitoring activities only as necessary to determine the degree of security provided to Government telecommunications and aid in countering their vulnerability. Such activities shall be conducted in strict compliance with current law, executive orders, and policy.

b. Government telecommunications systems are subject to COMSEC monitoring by duly authorized Government entities. The use of such systems by any person shall be construed to imply con-

sent to the monitoring for COMSEC purposes of communications carried over them.** Users of these systems must be properly notified in advance, in accordance with the guidelines in subparagraph 6.e., below, that their use of these systems constitutes consent to monitoring for COMSEC purposes. The Government shall not monitor telecommunications systems which are owned or leased by Government contractors for their own use without first obtaining the express written approval of the chief executive officer of the contractor organization (or his designee) and the written opinion of the General Counsel of the department or agency which is conducting the monitoring that procedures, such as those contained in subparagraph 6.e., below, have been implemented sufficiently to afford adequate notice to the contractor organization's employees.

c. The Government shall not monitor for COMSEC purposes the contents of any telecommunication when such monitoring would constitute electronic surveillance.

d. In accordance with procedures approved by the Attorney General, information acquired incidentally from Government telecommunications during the course of authorized COMSEC monitoring which relates directly to a significant crime will be referred to the military commander or law enforcement agency having appropriate jurisdiction. When taking such action, the General Counsel of the department or agency which is conducting the COMSEC monitoring shall be notified promptly. The results of COMSEC monitoring may not be used in a criminal prosecution without prior consultation with the General Counsel of the department or agency which performed the monitoring.

e. The results of COMSEC monitoring shall not be used to produce foreign intelligence or counterintelligence, as defined in Reference e. However, the results of COMSEC monitoring of U.S. and Allied military exercise communications may be used for exercise intelligence purposes under procedures prescribed in applicable directives.

f. No department or agency may monitor the telecommunications of another department or agency for COMSEC purposes without the express prior written approval of a responsible official of the department or agency to be monitored, except as provided for in subparagraph 8.b.(2).

g. It is recognized that COMSEC monitoring operations conducted in a crowded telecommunications environment may result in the temporary acquisition of private communications. COMSEC monitoring shall be conducted in accordance with operational procedures which minimize the possibility that the contents of such telecommunications will be acquired. Such procedures shall be consistent with the guidelines contained herein and shall be endorsed by the General Counsel of the department or agency issuing the procedures.

** Consent to COMSEC monitoring is required of only one party to a conversation or transmission.

6. GUIDELINES FOR THE CONDUCT OF COMSEC MONITORING

a. COMSEC monitoring may be undertaken for the following reasons appropriate to the purpose described in paragraph 2., above:

(1) To collect operational signals needed to measure the degree of security being achieved by U.S. codes, cryptographic equipment and devices, COMSEC techniques, and related materials.

(2) To provide a basis from which to assess the types and value of information subject to loss through intercept and exploitation of Government telecommunications.

(3) To provide an empirical basis for improving the security of Government telecommunications against SIGINT exploitation.

(4) To assist in determining the effectiveness of Electronic Countermeasures/Electronic Counter-Countermeasures (ECM/ECCM) and cover and deception measures.

(5) To identify Government telecommunication signals that exhibit unique external signal parameters, signal structures, modulation schemes, radio fingerprints, etc., that could provide SIGINT elements of foreign powers the capability to identify specific targets for subsequent geopositioning and exploitation purposes.

(6) To provide empirical data to train users of Government telecommunications systems in proper COMSEC techniques and measures.

(7) To evaluate the effectiveness of COMSEC education and training programs.

(8) To train personnel and to test the capability of COMSEC monitoring equipment.

b. The following categories of telecommunications are not considered private for purposes of this Instruction. Accordingly, acquisition of the contents of any communications in these categories which may occur in the course of locating or examining Government telecommunications is not electronic surveillance.

(1) Commercial broadcast radio communications.

(2) Public safety, citizens band, amateur radio, and similar radio systems licensed by the Government for public use or access.

(3) Any communications in portions of the electromagnetic spectrum which are allocated by the Government for its own use.

c. No incidentally acquired private communication may be monitored beyond the point where a determination can reasonably be made that it is private. A record of the acquisition may be kept for signal identification and avoidance purposes; such a record may describe the signal parameters (frequency, modulation, type, and timing) but may not identify the contents of the communication.

d. Contents of any private communication may not be deliberately acquired as part of a procedure for locating, identifying, or monitoring a Government communication.

e. Notice of the existence of COMSEC monitoring in conformance with subparagraph 5.b., above, can be accomplished by any of the following means or any combination thereof which the legal coun-

sel of the affected department or agency considers legally sufficient to achieve proper notification in terms of content, prominence, and specificity.

(1) Decals placed on the transmitting or receiving devices.

(2) A notice in the daily bulletin or similar medium.

(3) A specific memorandum to users.

(4) A statement on the cover of the official telephone book or communications directory.

(5) A statement in the standing operating procedures, communications-electronics operating instructions, or similar documents.

7. CONTROL OF MONITORING RECORDS AND EQUIPMENT

a. All reports, logs, and material produced in the course of COMSEC monitoring will be afforded protection commensurate with the classification of the information and the sensitivity of the monitored activity. Reports or material produced from COMSEC monitoring which identify security weaknesses of the monitored activity will be classified at least confidential and downgraded to unclassified when security weaknesses are corrected.

b. Interim and final reports may be disseminated only to the extent necessary for COMSEC purposes except as provided for in subparagraph 5.d., above. These reports shall not contain any information extraneous to COMSEC purposes, or names of individuals or sufficient data to identify the source except in an official capacity, e.g., "the radio operator on watch." Dissemination controls should be expressly stated on each report.

c. All COMSEC monitoring recordings and written records, logs, and notes shall be destroyed as soon as operationally feasible.

d. Except as provided for in subparagraph 5.d., above, no information extraneous to COMSEC purposes will be recorded, reported, noted, logged, or filed. If within the capabilities of COMSEC monitoring equipment, any such information that is inadvertently acquired shall be expunged upon recognition. All monitoring records shall be reviewed for identification and expungement of extraneous information within a reasonable time after they are created.

e. Access to and dissemination of COMSEC monitoring recordings or written records, reports, logs, and notes shall be limited to that which is necessary for COMSEC purposes. No access to, or dissemination of, such materials beyond COMSEC operational elements shall be allowed until such material is reviewed to determine that it contains no information extraneous to COMSEC purposes.

f. COMSEC monitoring equipment systems shall be safeguarded to prevent unauthorized access and use.

8. RESPONSIBILITIES

a. Heads of departments and agencies shall:

(1) Provide for and conduct COMSEC monitoring operations as they deem appropriate, subject to the provisions of law, executive orders, policy, and this Instruction.

(2) Develop procedures for the conduct of COMSEC monitoring, consistent with the policy and guidelines herein, in col-

laboration with the Director, NSA. Such procedures shall be approved by the Attorney General.

b. The Director, NSA shall:

(1) Advise and assist other departments and agencies in establishing their operating procedures to implement this Instruction.

(2) Monitor fielded Government cryptography as necessary to discharge his responsibilities under the National COMSEC Directive, provided that prior notice will be given to the organization whose encrypted telecommunications are to be monitored. No monitoring will be conducted which results in or affords a substantial likelihood that the plaintext of a communication, other than short-duration plaintext operator conversations associated with establishing a secure condition, will be acquired without the prior approval of the entity whose telecommunications are to be monitored.

LINCOLN D. FAURER,
Lieutenant General, USAF, Director.

Section 108 contains three subsections. Subsection (a) amends chapter 205 of title 18 to add a new section 3117. This section provides that if a court is authorized to issue a warrant or other order for the installation of a mobile tracking device, such an order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction. It should be noted that, unlike a mobile interception device, a tracking device may be utilized outside the United States once the device is installed within the court's jurisdiction. Subsection (b) of the proposed section contains a definition. "Tracking device" is defined to mean an electronic or mechanical device which permits the tracking of the movement of a person or subject.

Subsection (b) of section 108 contains a technical amendment to amend the table of chapters.

The provisions of this section are intended to permit the installation of tracking devices which may move from district to district. The section does not affect the legal standard for the issuance of orders authorizing the installation of each device. *See generally United States v. Karo*, 104 S. Ct. 3296 (1984) (a search warrant not required where the owner consents to installation); *United States v. Knotts*, 460 U.S. 276 (1983) (installation of a beeper on a container to follow on a public roadway does not violate the Fourth Amendment). The Court in *Karo, supra*, did find that if investigators used a beeper to determine whether the beepered object is in a private location, a warrant is required. *See Fishman, Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo and the Questions Still Unanswered*, 34 CATH. UNIV. L. REV. 277 (1985).

Section 109 adds two new offenses to section 2232 of title 18. The first new offense is to warn or give notice to a person that they are the subject of an act of interception under title 18. The elements of the offense require that the defendant have knowledge [41] that the federal law enforcement or investigative officer has been authorized or has applied for an interception order. The defendant need

[41] See House Report 96-1396, *Criminal Code Revision Act of 1980* at 82-86.

not know that such an application was under a particular chapter of federal law, rather, only that such application or order was under federal law. The defendant must engage in conduct of giving notice of the possible interception to the person who was or is the subject of the interception. *See* House Report 96-1396 at 82-86. Finally, the defendant must be shown to have engaged in such conduct with a specific motive such as to obstruct, impede or prevent the interception. Finally, the offense also includes attempts to engage in the offense.

The penalty for a violation of this new offense is a possible prison term of up to five years, a fine under this title, or both.

The second new offense set forth in section 109 is to warn the subject of an act of electronic surveillance under the Foreign Intelligence Surveillance Act (FISA). The elements of the offense are identical except that that type of surveillance order is governed by a different statute (FISA) and that statute authorizes a slightly different type of surveillance activity. The penalties for this offense are the same as the aforementioned offense.

Section 110 provides a new section 2521 in title 18. This new section adds to the existing panoply of criminal and civil remedies by authorizing the Attorney General to obtain an injunction to prevent felony level violations of this chapter. This provision is modelled after a similar statute (injunctions against fraud) enacted by Congress in the Comprehensive Crime Control Act of 1984, Public Law 98-473, *see also* Senate Report 97-307 at 1267. This section directs the court to proceed as soon as practicable to the hearing and determination of the matter. This section also provides that preliminary relief can be granted to prevent injury during the pendency of the action. A proceeding under this section is governed by the Federal Rules of Civil Procedure (particularly Rule 65). In the event, however, that an indictment has been returned against the respondent then discovery by both sides is limited to that permissible under the Federal Rules of Criminal Procedure.

Section 111 provides the effective date for the amendments made by this title. Subsection (a) of this section provides the general rule, that except as provided in subsection (b) the amendments made in this title take effect 90 days after the date of enactment. In the case of conduct pursuant to a court order or extension such amendments only apply with respect to court orders or extensions made after this title takes effect. The exception found in subsection (a) is written to permit the continuation under the old law rules of interceptions authorized under such rules. Because ongoing investigations may involve lengthy interceptions, any new order or extension of an order made after the general effective date will be governed by the new law rules.

Subsection (b) of section 111 provides a special rule for state authorization of interceptions. This special effective date rule is necessary because the provisions of chapter 119 of title 18 supersede previous state laws, to the extent that they exist, with respect to electronic communications. Under the provisions of chapter 119 the various states must enact statutes which are at least as restrictive as the provisions of chapter 119 before they can authorize their state courts to enter such interception orders. Because of the massive number of changes made in chapter 119 by this title in relation to electronic communication, it seemed appropriate to grant the states sufficient time to modify their laws accordingly. The special rule, in essence, gives the states two years to bring their laws into conformity with these amendments of chapter 119 of title 18. It is possible that state laws will not need be changed to accommodate revisions on interceptions of wire or oral communications. Any such changes would also benefit from the two-year delayed effective date.

TITLE II—STORED AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORD ACCESS

Section 201 amends title 18 by adding a new chapter 121 which consists of ten new proposed sections. These sections are discussed below.

Proposed section 2701 provides a new criminal offense. The offense consists of either: (1) intentionally accessing, without authorization, a facility through which an electronic communication service is provided or (2) intentionally exceeding the authorization of such *facility*. In addition, the offense requires that the offender must, as a result of such conduct, *obtain, alter* or prevent unauthorized access to a wire or electronic communication while it is in electronic storage in such a system. The term "electronic storage" is defined in section 2510(17) of title 18. Electronic storage means any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof and the storage of such communication by an electronic communication service for purposes of back-up protection of such communication.

Section 2701(a) makes it an offense intentionally to access without authorization, or to exceed an authorization to access, an electronic communication service and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system. This provision addresses the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public. The Committee recognizes, however, that some electronic communication services offer specific features, sometimes known as computer "electronic bulletin boards," through which interested persons may communicate openly with the public to exchange computer programs in the public domain and other types of information that may be distributed without legal constraint.

It is not the Committee's intent to hinder the development or use of "electronic bulletin boards" or other comparable services. The Committee believes that where communications are readily accessible to the general public, the sender has, for purposes of Section 2701(a), extended an "authorization" to the public to access those communications. A person may reasonably conclude that a communication is readily accessible to the general public if the telephone number of the system and other means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy. To access a communication on such a system should not be a violation of the law.

Some communication systems offer a mixture of services some, such as bulletin boards, which may be readily accessible to the general public, while others—such as electronic mail—may be intended to be confidential. Such a system typically has two or more distinct levels of security. A user may be able to access electronic bulletin boards and the like merely with a password he assigns to himself, while access to such features as electronic mail ordinarily entails a higher level of security (i.e., the mail must be addressed to the user to be accessible specifically). Section 2701 would apply differently to the different services. Those wire or electronic communications which the service provider attempts to keep confidential would be protected, while the statute would impose no liability for access to features configured to be readily accessible to the general public.

Section 2701(a) generally prohibits any person from intentionally accessing a wire or electronic communication system without authorization or in excess of authorization, and thereby ~~obtaining~~ access to a wire or electronic communication while it is in electronic storage in the system. An "electronic mail" service, which permits a sender to transmit a digital message to the service's facility, where it is held in storage until the addressee requests it, would be subject to Section 2701. A "voice mail" service operates in much the same way, except that the stored message takes the form of the sender's voice, usually in digital code. It would likewise be subject to Section 2701. Similarly, to the extent that a remote computing service is provided through an Electronic Communication Service, then such service is also protected.

A person found guilty of this new offense is subject to a maximum penalty as specified in subsection (b) of proposed section 2701. Subsection (b) provides a general rule that such an offense is punishable by a fine of $5,000 or imprisonment of not more than six months, or both. There are two exceptions to this general rule. If the offender has acted for purposes of commercial advantage, malicious destruction or damage, or private financial gain, the possible penalty is escalated to a fine of up to $250,000 and a prison term of up to one year or both. The second exception is to increase the potential jail term for second or subsequent offenders up to two years in prison.

In light of the importance of communications generally to interstate and foreign commerce, the prevention of unauthorized access to the systems used for such communication is a legitimate federal concern. In some instances, unauthorized access to wire or electronic communications is undertaken for purposes of malice or financial advantage. Other instances, however, arise from the activities of computer amateurs, often called "hackers," whose goal is primarily the access itself. Still, "hacking" cannot be dismissed as a harmless prank; a hacker may stumble across sensitive or commercially useful information, and in any event invades the privacy of those whose communications are stored. It is thus important to prohibit unauthorized access even if undertaken without a malicious purpose or motive. Section 2701(b)(1) does, however, specify higher penalties for unauthorized access committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain.

Subsection (c) of proposed section 2701 provides that this section does not apply with respect to conduct which is authorized by: (1) the provider of the service; (2) the user of the service; or (3) the provisions of sections 2703 or 2704 of this new chapter.

Proposed section 2702 provides general prohibitions on the disclosure of contents. This proposed section provides that a person or entity providing electronic communication services to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service. This prohibition is similar to that found in chapter 119 with respect to the divulgence of a wire or electronic communication during transmission. The term knowingly means that the defendant was aware of the nature of the conduct, aware of or possessing a firm belief in the existence of the requisite circumstances and an awareness of or a firm *belief* about the substantial certainty of the result. The conduct in question is the act of *disclosure*. The result is that the contents have been provided to another person or entity. The circumstances involved are that the person involved provides electronic communication services to the public and that the contents relate to a wire or electronic communication. Knowledge as to a circumstance includes willful blindness, *Model Penal Code* section 2.02. Comment at 129–30 (Tent. Draft No. 4, 1955); *United States* v. *Jewell*, 532 F.2d 697 (9th Cir.), *cert. denied*, 426 U.S. 951 (1976). The concept of "knowingly" does not include, however, "reckless" or "negligent" conduct. *See* HOUSE REPORT 96–1396 *at* 33–34 (for *a* definition of terms). This provision is aimed at proscribing the disclosure of stored wire and electronic communications. Subsection (b) contains the exceptions to this general rule.

Subsection (a)(2) of proposed section 2702 provides that a person or entity providing remote *computing* services to the public shall not knowingly *divulge the contents of* any communication which is *carried or maintained* on that service if certain conditions are met. The term "contents" as used in section 2702 is intended to encompass the substance, purport, effect or meaning of the communication. *Under* this interpretation, a service provider is allowed to divulge mailing lists that identify persons fitting broad demographic criteria. Unless otherwise authorized, service providers may not divulge to third parties information that profiles the activities of individual subscribers through the divulgence of the contents of a communication. The first condition is that the affected communication must be on behalf of and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from) a subscriber or customer of such service. The second condition is that the affected communication be solely for the purpose of providing storage or computer processing services to such subscriber or customer, so long as the provider is *not* authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing. The prohibitions of this subsection are also modified by the exceptions in subsection (b).

Section 2702(a) protects communications "received by means of electronic transmission from * * * a subscriber or customer of such service" and kept "solely for the purpose of providing storage or

computer processing services to such subscriber or customer * * *." In the case of either electronic mail or voice mail, the sender—a user of the service—has necessarily authorized the addressee's access to the message. The addressee's acquisition of the message is therefore clearly within the contemplation of section 2701(c). Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. The Committee intends that, in leaving the message in storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, and that such communication should continue to be covered by section 2702(a)(2).

Section 2702(a) generally prohibits the provider of a wire or electronic communication service to the public from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient of such communication, or an agent of such addressee or intended recipient. Similarly, section 2511(3) of title 18, as amended, prohibits such a provider from divulging the contents of a communication while it is in transmission. Neither provision, however, nor any other provision in the Act, is intended to affect any other provision of federal law that prohibits the disclosure of information on the basis of the content of the information, such as the Fair Credit Reporting Act.

The application of sections 2701(a) and 2511(3) is limited to providers of wire or electronic communications services. There are instances however, in which a person or entity both acts as a provider of such services and also offers other services to the public. In some such situations, the bill may allow disclosure while another federal requirement, applicable to the person or entity in another of its roles, prohibits disclosure. The Committee intends that such instances be analyzed as though the communication services and the other services were provided by distinct entities. Where a combined entity in its non-provider role would not be allowed to disclose, the appropriate outcome would be non-disclosure.

One example of such an instance could arise under the Fair Credit Reporting Act, 15 U.S.C. 1681b, which limits the circumstances under which consumer reporting agencies may disclose certain information relating to consumers. An entity may perform a consumer reporting agency function, and may also provide wire or electronic communication services to the public. Such an entity might provide itself with electronic communication services, including the storage of data relating to consumers. Sections 2701(a) and 2511(3) have no effect on the entity's role as a consumer reporting agency, and in that role the entity must comply with the disclosure limitations of the Fair Credit Reporting Act.

Section 2702(a)(2) prohibits the provider of a remote computing service to the public from knowingly divulging the contents of any communication carried or maintained on the service on behalf of, and received by means of (or created from communications received by means of) electronic transmission from a subscriber or customer of the service, and carried or maintained solely for the purpose of providing such service to the subscriber or customer. This provision reflects the rapidly growing importance of information storage and processing to the Nation's commerce. Today, the subject matter of commerce increasingly is information in electronic form and the processing of information itself has become a major industry. The secure storage of electronic information has thus become as important to the commercial system as the protection of paper records. Accordingly, where an electronic communication is transmitted by a subscriber or customer to such a service, and is stored on the subscriber's behalf solely for the purpose of providing storage or computer processing services to the subscriber, the Committee intends that the communication—together with the products of any processing that the service performs for the customer—remain available only to the subscriber and to the persons he designates, with certain exceptions enumerated in Section 2702(b).

Section 2702 specifies that a person or entity providing wire or electronic communication service to the public may divulge the contents of a communication while in electronic storage by that service with the lawful consent of the originator or any addressee or intended recipient of such communication. The Committee emphasizes that "lawful consent," in this context, need not take the form of a formal written document of consent. A grant of consent electronically would protect the service provider from liability for disclosure under Section 2702. Under various circumstances, consent might be inferred to have arisen from a course of dealing between the service provider and the customer or subscriber—e.g., where a history of transactions between the parties offers a basis for a reasonable understanding that a consent to disclosure attaches to a particular class of communications. Consent may also flow from a user having had a reasonable basis for knowing that disclosure or use may be made with respect to a communication, and having taken action that evidences acquiescence to such disclosure or use—e.g., continued use of such an electronic communication system. Another type of implied consent might be inferred from the very nature of the electronic transaction. For example, a subscriber who places a communication on a computer "electronic bulletin board," with a reasonable basis for knowing that such communications are freely made available to the public, should be considered to have given consent to the disclosure or use of the communication. If conditions governing disclosure or use are spelled out in the rules of an electronic communication service, and those rules are available to users or in contracts for the provision of such services, it would be appropriate to imply consent on the part of a user to disclosures or uses consistent with those rules.

Section 2702(a) specifies that a person or entity providing a wire or electronic communication service or remote computing services to the public shall not knowingly divulge the contents of any communication while in electronic storage by that service to any person or entity other than the addressee or intended recipient of such communication or an agent of such addressee or intended recipient. Under Section 2702(b), disclosure to any other person requires the consent of the originator or any addressee or intended recipient of the communication. Under some circumstances, however, a customer of or subscriber to a wire or electronic communication service may place a communication on the service without specifying an addressee. The Committee intends, in that situation,

that the communication at a minimum be deemed addressed to the service provider for purposes of Section 2702(b). Because an addressee may consent to the disclosure of a communication to any other person, a service provider or system operator, as imputed addressee, may disclose the contents of an unaddressed communication.

A person may be an "intended recipient" of a communication, for purposes of Section 2702, even if he is not individually identified by name or otherwise. A communication may be addressed to the members of a group, for example. In the case of an electronic bulletin board, for instance, a communication might be directed to all members of a previously formed "special interest group" or, alternatively, to all members of the public who are interested in a particular topic of discussion. In such an instance, the service provider would not be liable for disclosure to any person who might reasonably be considered to fall in the class of intended recipients.

Subsection (b) of proposed section 2702 provides six distinct exceptions to the general limitations on divulgence contained in subsection (a). The first exception is with respect to divulgence to an addressee or intended recipient of a communication or an agent thereof. Section 2702(b) which places limits on disclosure. In connection with disclosures made pursuant to section 2702(b)(4), these limitations apply along the agent claim, the second exception is divulgence authorized by statutory provisions in either chapter 119 or this chapter. The third exception is divulgence with the lawful consent of the originator, addressee, or intended recipient (or subscriber in the case of remote computer service). The fourth exception is to permit divulgence to a person who is involved in forwarding the communication to its destination. The fifth exception permits divulgence necessarily incident to the rendition of such services or to the protection of the rights or property of the provider of the services. The terms "rights" and "property" here refer to such rights as intellectual property rights, the right to be free from the theft of services. The term is not intended to be read as to permit a provider to contract with an unauthorized party an obligation to divulge all stored messages, without notice to or any consent from the originator of the message, and then to claim that such divulgence is to protect the rights in such a contract. The sixth exception authorizes the divulgence to a law enforcement agency if the contents of the communication were inadvertently obtained and appear to pertain to the commission of a crime. This exception is intended to be read narrowly. A systematic practice of reviewing stored communications to look for evidence of a crime could not qualify as inadvertent.

Proposed section 2703 contains the procedural requirements for the government to obtain access to electronic communications in storage and transactional records relating thereto. Proposed section 2703 contains four subsections.

Subsection (a) sets forth the requirements which must be met before the government may obtain access to the contents of a non-voice wire communication or an electronic communication in storage. As a general rule the government must obtain a search warrant. The contents of the voice portion of a wire communication in storage such as with "voice mail" may not be obtained under this

section. Under the provisions of chapter 119 of title 18 apply. The general rule applies to electronic communications which have been in electronic storage for 180 days or less. The government is, however, permitted to use alternative means of obtaining access if the communication has been in storage for more than 180 days. For this second category of stored records, the government may use an administrative subpoena authorized by federal or state law or a federal or state grand jury subpoena or a court order under subsection (d) of this section, provided that the customer obtains notice. There is an exception for the notice required for this alternative means, and that exception is set forth in proposed section 2704.

The Committee required the government to obtain a search warrant because it concluded that the contents of a message in storage were protected by the Fourth Amendment. The reasons for such a conclusion are set forth more completely earlier in this report. The Committee recognized that electronically stored communications can be of two types. The first type of stored communications are those associated with transmission and incident thereto. The second type of storage is of a back-up variety. Back up protection preserves the integrity of the electronic communications system and to some extent preserves the property of the users of such a system. Most—if not all—electronic communications systems (such as electronic mail systems), however, only keep copies of messages for a few months. To the extent that the record is kept beyond that point it is closer to a regular business record maintained by a third party and, therefore, deserving of a different standard of protection.

Subsection (b) sets forth the procedures the government must use before it can obtain access to the contents of any electronic communication held by a provider of remote computing services. The government may proceed using any of three alternative means of access. The government may, without providing the required notice to the subscriber or customer, obtain a search warrant. The government may also choose to obtain access by giving notice to the subscriber or customer, and using either (a) an administrative summons authorized by federal or state law or a grand jury subpoena; or (B) a court order under subsection (d). The requirement that the state law authorize the use of a grand jury subpoena or administrative summons for purposes of obtaining access to such records—and the parallel requirement in subsection (d) that a court order be obtained under certain standards—are intended to apply the relevant state law with respect to the legal standard such officials must meet with respect to access to those records. Thus, to the extent that a state law or State Constitution requires that a court order based on a standard other than relevance be obtained by a state government official before such official can obtain access to the type of records protected by this chapter, then that law would preclude the use of the provisions of this section with respect to state government officials. Thus, state laws such as those found in Colorado, California, New Jersey and Pennsylvania would remain unaffected with respect to access by state government officials. *See* discussion of records access, *supra*. To the extent that such access is sought by a federal official under the conditions specified under this section, then state law is overridden by virtue of the Suprema-

cy Clause. Examples of such federal legal authority include administrative summons used by the Drug Enforcement Administration, 21 U.S.C. 876, and by the Internal Revenue Service, 26 U.S.C. 7609. Nothing in this authorization eliminates any notice which may be required under other laws. *See, e.g.*, 26 U.S. 7609. The notice required under subsection (b)(1)(B) (i) and (ii) may be dispensed with if the conditions of section 2704 have been met. The type of records to which the provisions of subsection (b) apply are set forth in subsection (b)(2).

The type of electronic communication held by a remote computing service which is protected from governmental access is limited by certain preconditions. The communication must be on behalf of a subscriber or customer of a remote computing service and such communication must have been given to the remote computer service under narrow conditions. The narrow conditions are that the communication must have been received in a certain form (i.e by means of electronic transmission or similar means). In addition, the communication must have been surrendered solely for the purpose of providing storage or computer processing services to the subscriber or customer, and the provider may not be authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing

Subsection (c) sets forth the rules under which the government may require the provider of electronic communications services or remote computing services to disclose a record or other transactional information concerning a subscriber or customer (other than the contents of a communication) The type of records involved are billing records and telephone toll records (including the record of long distance numbers and message unit detailing information). The government need not provide notice to the subscriber or customer before it seeks access to these types of records. On the other hand, the government must use one of three sets of authorized procedures. The government can rely on administrative subpoenas or grand jury subpoenas to the extent that such processes are legally authorized. Alternatively, the government can use a search warrant. Finally, the government can seek a court order directing the disclosure of such records. If a court order is sought then the government must meet the procedural requirements of subsection (d).

Subsection (d) provides that the government shows that there is reason to believe that the contents of an electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. The only contents which can be sought using the court order option are, of course, those stored for more than 180 days.

It should be noted that when the government is required to give notice to the customer or subscriber that the purpose of such notice is to provide the subscriber or customer with an opportunity to contest the propriety of such a disclosure. The customer or subscriber has standing to raise any legitimate defense to such disclosure including any constitutional claims under the First, Fourth, Fifth or Fourteenth Amendments, any claims of privilege, and any available defenses to improperly issued subpoenas. Whether any of these claims are accepted by the court before whom the application is pending will depend on the facts of a given case and the state of the law at the time

Proposed section 2704 sets forth in four subsections the procedures governing back-up copy preservation.

Subsection (a)(1) provides that when the government is seeking access to remote computing service information on records under section 2703(b)(2) that the government can seek and obtain the assistance of the provider in preserving the information or records sought. The government may, under this subsection include with its subpoena or court order a request that the provider create or generate a back-up copy of the requested records or information. The provider is directed to create a back-up copy as soon as practicable consistent with its regular business practices. Thus, if a service promotor maintains back-up copies as part of its regular business activities, it does not have to create a new copy. The provider is directed not to inform the customer or subscriber of this activity. After the copy has been made the provider is directed to inform the governmental entity seeking the copy that it has complied with the request. Finally, this subsection sets as an outside limit for the creation of a back-up copy of two business days.

Subsection (a) provides that once the governmental entity has received confirmation that it shall notify the customer or subscriber within three days, unless such notice is delayed under the terms of proposed section 2704(c). At this point the provider is also free to notify the subscriber or customer unless prohibited under subsection (b) of proposed section 2705.

Subsection (a)(3) provides that the provider shall not destroy a back-up copy generated under this section until the latter of the delivery of the information or the resolution of any proceedings related to the access question. If the governmental entity has notified the customer or subscriber and that person has not challenged the requested access then after the passage of fourteen days the provider may make the disclosure. Subsection (a)(5) provides that a governmental entity may only seek to require the creation of a back-up copy under subsection (a)(1) if in its sole discretion there is reason to believe that notification under section 2703 may result in destruction or tampering with the information sought. This determination that notification under section 2703 may result in hampering with or destruction of evidence on similar adverse results by the governmental entity is not subject to challenge by the subscriber or customer or service provider.

Subsection (b)(1) of proposed section 2704 provides that within fourteen days after receipt of notice by the government that a back-up copy has been requested the subscriber or customer may move to quash or vacate. This subsection sets forth the procedural details of such proceedings. The challenger must service the governmental entity and provide written notice to the provider of the challenge. A motion to vacate shall be made in the court which issued the original order. Similarly, a motion to quash shall be made in the appropriate state or federal court. The motion or application under this subsection must establish that the challenger is the relevant customer or subscriber. The challenger must also set forth reasons why the records being sought are not relevant to a legitimate law enforcement inquiry or that some other legal defect exists such as failure by the government to comply with the requirements of this chapter.

Subsection (b)(2) sets forth service of process rules. Service under this section may be made by registered or certified mail to the appropriate governmental entity.

Subsection (b) provides that the government shall be directed to file a sworn response if the challenger has met the requirements of this subsection. The governmental response may be filed *in camera* if appropriate. If the court cannot on the basis of the initial set of papers determine the challenge, then additional proceedings may be conducted. Any additional proceedings and a decision on the challenge shall occur as rapidly as feasible, *i.e.* within 7 calendar days in all but the most unusual circumstances.

Subsection (b)(4) provides that if the court determines that the challenger is not the subscriber or the customer affected does not have legal standing to contest the disclosure then the court shall deny the motion or application. Denial is also directed if the court finds that the information sought is relevant to the legitimate law enforcement inquiry. On the other hand, if the challenger has standing and can show either lack of relevance or non-compliance with the procedural requirements of this section then the court may vacate the order or quash the subpoena.

In the event that there is no indictment then the person whose records are involved may move for the return of the records.

Subsection (b)(5) provides that a court order denying a motion or application under this section shall not be deemed a final order and therefore no interlocutory appeal may be taken from such a denial. Obviously, nothing precludes a customer or subscriber who is later the subject of a criminal proceeding from raising these issues again subject to the sanctions limitation of section 2708.

Proposed section 2705 (a) provides the conditions wherein delay of any required notification may be achieved. Under subsection (a)(1) a governmental entity may request a delay of notification for a period of up to 90 days if the governmental entity convinces the court that there is reason to believe that such notification will produce adverse results as described in subsection (a)(2) of proposed section 2704. Alternatively, where an administrative or grand jury subpoena is obtained, delay may be achieved if a supervisory official files a written certification that such delay is necessary to avoid adverse results. In the second case, the delay in notice can only last initially for a period of up to 90 days.

Subsection (a)(2) sets forth the adverse results which can trigger the delay of notification set out in paragraph (1) of this section. There are five enumerated adverse results: (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses (including victims of any crimes); and (5) otherwise seriously jeopardizing an investigation or unduly delaying an ongoing trial.

Subsection (a)(3) requires the government to maintain a true copy of the certification required under paragraph (1)(B) of this section.

Subsection (a)(4) provides that extensions of up to 90 days may be made of the notification so long as the original requirements of this section are met with respect to the extension.

Subsection (a)(5) provides that upon the expiration of any period of delay the governmental entity which has obtained the information shall serve upon the customer or subscriber a copy of the process used to obtain the information. Service under this subsection can be by first class or registered mail. In addition, the government entity must also include a notice that states with reasonable specificity the nature of the law enforcement inquiry. Such notice shall also tell the customer or subscriber when the information was furnished, that the notification was delayed, who authorized the delay and under what provision of law.

Subsection (a)(6) defines, for purposes of this subsection, the term "supervisory official". Such term means the investigative agent or assistant investigative agent in charge or an equivalent official in the investigating agency's headquarters or regional office. The term also means the chief prosecuting attorney or first assistant prosecuting attorney or an equivalent official in a regional or headquarters office.

Subsection (b) of this section provides a procedure for the government to preclude the service provider from notifying the customer or subscriber in a narrow set of circumstances. First, such preclusion may only be obtained in instances where the government is not required to notify, or where the government has obtained the authority to delay notification. Second, a preclusion of notification must be granted by a court of competent jurisdiction. The final requirement is that the court be convinced that there is reason to believe that adverse results set forth in subsection (b) will occur if notification is given.

Sections 2702, 2703 and 2704 affect the contents of communications in storage or where information is being maintained for a subscriber or customer in a remote computing facility. New technologies have created capacities for storage of communications and the single prohibition of interception is not sufficient to cover this record-type aspect of communication. A person who subscribes to an electronic mail service may not realize it, but that service likely maintains a record of all system transactions for a period of time, usually six months under current industry practice. Even if the subscriber reads the message and discards or deletes it, the system maintains it as a backup copy for system maintenance and integrity purposes. These records are retrievable and the Committee intends that subscribers and customers be afforded some protection as to these records. Therefore, a provider of electronic communications to the public such as an electronic mail service may not disclose the contents of stored communications unless one of the statutory exceptions in 2702(b) apply. One of the exceptions, (b)(2), applies where the government has requested access either under section 2703 or 2516.

The Committee has sought to add significant protection to the provision of remote computing services where the contents of communications are electronically transmitted to such service. In most instances, records maintained by third parties have no special privacy or confidentiality protection. The United States Supreme Court has held that an employer's wage records are not subject to the assertion of interest by an employee. *Donaldson v. U.S.*, 400 U.S. 517 (1971). Similarly, in *Miller v. U.S.*, 425 U.S. 435, 1976, the

Court held that an individual has no standing to challenge the disclosure to government of records maintained by banks for their checking account customers. In *Donaldson*, the records sought were the wage records of the employer and were not kept or maintained for the employee. In *Miller*, the bank customer used the bank as an agent to facilitate financial transactions. The records of a checking account were evidence of a public transaction and the disclosure of them to a grand jury did not violate any constitutional rights of bank customers.

These cases were studied extensively by the United States Privacy Protection Study Commission and by the Congress. The Report of the Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977). The Privacy Commission recommended that individuals have enforceable rights to limit the disclosure of records maintained about them for third parties. The Congress acted upon these recommendations in the financial records area by enacting the Right to Financial Privacy Act in 1978 12 U.S.C. 3400 et seq. That statute in overruling *Miller* requires federal government agencies to use legal process to obtain bank records and allow the bank customer to seek to quash such process.

Last term the Congress extended this type of record privacy protection to records maintained by cable operators. In the Cable Communications Privacy Act of 1984, cable companies in the provision of one-way and two-way services are restricted in the type of information they may disclose about subscribers. Public Law 98-549. Moreover, the legislation, like the Right to Financial Privacy Act, requires the government to obtain records only through a court order or legal process with an opportunity to the subscriber to appear and contest the disclosure of the information.

This Committee is convinced that the subscribers and customers of remote computing services should be afforded a level of confidence that the contents of records maintained on their behalf for the purpose of providing remote computing services will not be disclosed or obtained by the government, unless certain exceptions apply or if the government has used appropriate legal process with the subscribers or customers being given an opportunity to protect their rights.

Proposed section 2706 contains two subsections. Subsection (a) provides that a governmental entity obtaining the contents of communications, records or other transactional information under section 2702, 2703 (with certain exceptions) or 2704 of this title shall pay the person or entity providing such information a fee. The fee under this section shall be reimbursement for such costs as are reasonably necessary and which have been directly incurred in search for, assembly, reproducing or otherwise providing such information. Included in such costs are delivery costs. Also included are any costs due to the necessary disruption of the normal operations of a provider.

Subsection (a) exempts from the reimbursement provisions certain types of records unless the requirement of subsection (c) are met. The type of records involved are telephone toll records and telephone listings. These records are excluded, because for the most part the government has not traditionally paid for such information. Nothing in this exclusion, however, affects the government's obligation to pay for information through other requests (i.e. requests other than under this chapter). Thus, if a government agent uses a telephone to request information assistance then compensation will be due. Similarly any court appearances in connection with such an information request would be covered elsewhere.

Subsection (b) provides that the amount of the fee provided by subsection (a) of this section shall be either mutually agreed upon or determined by the appropriate court. The subsection specifies which court would be appropriate.

Subsection (c) of proposed section 2703 provides that a court may, upon the request of a person providing information, request an appropriate court to order reimbursement for payment related to expenses incurred in connection with the searching for, reproducing, or transporting books, papers, records, or other information or data required or requested to be produced. *See, e.g.,* 12 U.S.C. 3415. The provider may obtain such reimbursement if the information required is voluminous or otherwise causes an undue burden on the provider. The Committee expects that the Department of Justice will, by *regulation* (subject to notice and comment), promulgate written criteria *to guide the parties and the* courts with respect to the meaning of the terms "voluminous" and "undue burden". The Committee hopes that the uniform application of regulations will reduce the need to rely on judicial intervention to resolve reimbursement disputes. The most important factor to examine is the nature of current and past practice in this area. To the extent that the request exceeds the nature and scope of information usually sought without compensation then the reimbursement provisions would come into play.

Proposed Section 2707 contains five subsections. Subsection (a) provides a civil cause of action for any subscriber or customer who has been aggrieved by a knowing or intentional violation of this chapter. Recovery may be had under this section against a person or entity who violated the provisions of this chapter. This includes governmental entities who have violated the provisions of this chapter. Relief as may be appropriate may be awarded under this section but includes preliminary and other equitable relief, declaratory relief, damages and reasonable attorney's fees and other litigation costs reasonably incurred. Subsection (c) provides the measure of damages under this section. Damages include actual damages, any lost profits but in no case less than $1,000.

Subsection (d) sets forth defenses to civil actions. This subsection provides that good faith reliance on a lawful order shall be a complete defense to any civil or criminal action brought under this chapter or any other law. The types of lawful orders are set forth as (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization, (2) a request of any investigative or law enforcement officer under section 2518(7); or (3) a good faith determination that section 2511(3) of this title permitted the conduct complained of.

Subsection (e) provides the statute of limitations. Under this subsection a civil action may not be commenced later than two years after the date upon which the claimant first discovered or had reasonable opportunity to discover the violation.

Proposed section 2708 provides that the remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter. See discussion of section 101(e) of the bill, *supra*.

Proposed section 2709 contains provisions relating to counterintelligence access to telephone toll and transactional records. Subsection (a) provides that a communications common carrier or an electronic communication service provider shall comply with a request made for telephone subscriber information and toll billing records information or electronic communication transactional records when such a request is made by the Director of the Federal Bureau of Investigation under subsection (b) of this section. Subsection (b) provides that the Director of the FBI (or an individual within the FBI designated for that purpose by the Director) may request any such information and records if there is a certification that the information sought is relevant to an authorized foreign counterintelligence investigation and that there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power (as those terms are defined in the Foreign Intelligence Surveillance Act of 1978).

Subsection (c) provides that a communications common carrier or service provider (including officers, employees and agents) shall not disclose to any person that the FBI has sought or obtained such information or records.

Subsection (d) provides that the FBI may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign counterintelligence collection and foreign counterintelligence investigations conducted by the FBI, with respect to dissemination to an agency of the United States. Any disclosure to a United States agency can only be made if the information is clearly relevant to the authorized responsibilities of such agency.

Subsection (e) provides that the Director of the FBI shall fully inform the House and Senate intelligence committees concerning all requests made under this section.

Proposed section 2910 contains definitions used in this chapter. As a general rule, the terms used in this new chapter have the same definitions as such terms have when used in chapter 119. The term "remote computing service" means "the provision to the public of computer storage or processing services by means of any electronic communication system." Remote computing services is not intended to apply to computer services offered by the various telephone company central offices in connection with the routing of telephone calls (such as speed dialing, call forwarding, and three-way dialing). Computer storage means all types of electronic or magnetic storage, including storage in the memory of a computer.

Section 201(b) contains a clerical amendment to amend the table of chapters to add a new title for chapter 121.

Section 202 of the bill contains the effective date. For this title and the amendments made by this title, the effective date is 90 days after the date of enactment. In the case of conduct pursuant to a court order or extension, it will apply only with respect to court orders or extensions made after this title takes effect.

TITLE III—PEN REGISTERS

This title contains one section and two subsections of the bill. Section 301(a) adds six new sections to title 18 relating to pen registers.

Proposed section 3121 contains three subsections. Subsection (a) contains a general prohibition on pen register use. The subsection provides that no person shall install or use a pen register without first obtaining a court order under section 3123 or under the Foreign Intelligence Surveillance Act.

Subsection (b) contains exceptions to the general list of prohibitions. The subsection provides that the prohibitions do not apply with respect to the use of a pen register by a provider of electronic or wire communication service if either of two conditions are met. The first condition is that such use relates to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of the service or unlawful use of service.

The second permissible condition for the use of a pen register is to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or user of that service, from fraudulent, unlawful or abusive use of service, or with the consent of the user of that service.

Subsection (c) provides that penalty for knowingly violating subsection (a). The penalty is a fine under this title or imprisonment of up to one year, or both.

The absence of any specific civil cause of action for violations of proposed chapter 206 was purposeful; therefore, no private cause of action should be implied under this chapter.

Proposed section 3122 provides the procedures for making an application for a pen register order. Under subsection (a) an attorney for the government may make an application for an order or an extension of an order authorizing or approving the installation and use of pen registers. The application shall be in writing under oath or equivalent affirmation to a court of competent jurisdiction. Subsection (a)(2) contains parallel provisions with respect to state applications. The phrase ". . . unless otherwise prohibited by State law" in this subsection makes clear that this law does not preempt any existing state laws with respect to installation and use of pen registers by state officials. To the extent that state law currently provides that a pen register may only be installed or used by a state official based on some other, higher standard of proof, that law will continue in effect with respect to such officials. *See People v. Sporleder*, 666 P. 2d 135 (Colo. Sup. Ct. 1983); Note, On Privacy, Pen Registers, and State Constitutions: The Colorado Supreme Court Rejects *Smith* v. *Maryland*, 15 Tol L. Rev. 1466 (1984); *People v. McCunes*, 51 Cal. App. 3d 487 (1975) Subsection (b) provides what factual details need to be provided in the application. The application shall include the identity of the attorney for the federal or state government and the identity of the applicant making the application, and a certification by the applicant that the information

likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency.

Proposed section 3123 contains four subsections. Subsection (a) provides that upon an application the court shall issue an *ex parte* order authorizing the installation and use of a pen register within the jurisdiction of the court if the court finds that the government attorney has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. This provision does not envision an independent judicial review of whether the application meets the relevance standard rather the court needs only to review the completeness of the submitted certification.

Subsection (b) sets forth the contents of the order for a pen register, authorization or installation. The order is required to specify (1) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register is attached; (2) the identity, if known, of the person who is the subject of the criminal investigation; (3) the number and, if known, physical location of the telephone line to which the pen register is attached; and (4) a statement of the offense to which the information likely to be obtained by the pen register relates. In addition, the order shall direct, upon request, the furnishing of information facilities and technical assistance necessary to accomplish the installation of the pen register. The content of the order relating to cooperation is intended to codify the existing informal practice of cooperation between the telephone companies and the Department of Justice.

Subsection (c) provides that the time period of authorization of an installation and use of a pen register is 60 days, with possible extensions of 60 days.

Subsection (d) provides that an order authorizing or approving the installation and use of a pen register shall direct that the order be sealed, until otherwise ordered by the court. In addition, the order shall bar the disclosure of the existence of a pen register or an investigation to the listed subscriber, or to any other unauthorized person, unless or until otherwise directed by the court. Intentional violations of the non-disclosure provisions may be, in appropriate circumstances, punishable as contempt.

Proposed section 3124 contains two subsections. Subsection (a) provides that upon the request of an authorized person a provider of a wire communication service, landlord, custodian, or other person shall furnish such person with all information, facilities, and technical assistance necessary to effectuate the order unobtrusively and with a minimum of interference. The Committee assumes that the current practice of law enforcement officials installing and maintaining the pen register will continue. Subsection (b) provides that the persons giving assistance under this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance. This compensation provision is modeled after that which applies under chapter 119 of title 18 and is intended to be interpreted and implemented in a similar fashion.

Proposed section 3125 provides that the Attorney General shall annually report to the Congress on the number of pen register orders applied for by law enforcement agencies of the Department of Justice. Under a current order of the Attorney General statistics concerning pen registers are compiled. Memorandum from Assistant Attorney General, Criminal Division, Department of Justice, Phillip B. Heyman to all Investigative Agencies, dated Sept. 24, 1979 (Recording the number of investigations, number of persons affected and nature of the offenses). This section merely requires that this information be reformulated and submitted to the appropriate committees of the Congress. Obviously the greater the detail contained in these reports the less need there will be for supplemental activities. Therefore, it would be helpful to the Committee if these reports could indicate for which offenses pen registers are being used.

Proposed section 3126 contains definitions for this chapter. Subsection (a) contains the *definitions*. The term "communications common carrier" has the same meaning as is found in section 3(h) of the Communications Act of 1934. The term "wire communication" has the meaning set forth in section 2510 of this title. The term "court of competent jurisdiction" means a district court of the United States (including a magistrate of such court) or a United States Court of Appeals or a court of general jurisdiction of a State authorized to enter orders authorizing the use and installation of pen registers. The term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted for purposes of routing telephone calls, with respect to wire communications, on the telephone line to which such device is attached. The term does not include the contents of a communication, rather it records the numbers dialed. Such term does not include any device used by a provider of wire communication service for billing, or recording as incident to billing, for communications services provided by such provider. The term "attorney for the government" has the meaning given to that term by the Federal Rules of Criminal Procedure. The term "state" means a State, the District of Columbia, Puerto Rico, and other possession or territory of the United States.

Subsection (b) of this section contains a clerical amendment amending *the table of chapters*.

Section 302 contains the effective date. Subsection (a) provides that as a general rule the amendments made by this title shall take effect 90 days after enactment. In addition, in the case of conduct pursuant to a court order or extension, these amendments apply only with respect to court orders or extensions made after the title takes effect.

Subsection (b) contains special rules or exceptions. This subsection, in essence, gives states two years to bring their laws into conformity with these amendments to federal law.

New Budget Authority

In regard to clause (l)(3)(B) of rule XI of the Rules of the House of Representatives, the bill creates no new budget authority or increased tax expenditures for the Federal judiciary.

Inflationary Impact Statement

In regard to clause 2(l)(4) of rule XI of the Rules of the House of Representatives, the commitee feels that the bill will have no foreseeable inflationary impact on prices or costs in the operation of the national economy.

Federal Advisory Committee Act of 1972

The Committee finds that this legislation does not create any new advisory committees within the meaning of the Federal Advisory Committee Act of 1972.

Cost Estimate

In compliance with clause 7 of rule XIII of the Rules of the House of Representatives, the committee estimates that the costs which will be incurred in carrying out the provisions of the reported bill are accurately reflected in the Congressional Budget Office estimate.

Congressional Budget Office Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, June 18, 1986.

Hon. Peter W. Rodino, Jr.,
Chairman, Committee on the Judiciary, House of Representatives, Rayburn Office Building, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has reviewed H.R. 4952, the Electric Communications Privacy Act of 1986, as ordered reported by the House Committee on the Judiciary, June 10, 1986. CBO estimates that enactment of this legislation will result in no significant cost to the federal government and no cost to state or local governments.

H.R. 4952 makes a number of amendments to Title 18 of the United States Code concerning access to electronic communications. Title I of the bill establishes penalties for the unlawful interception or disclosure of electronic communications, provides for the recovery of civil damages for persons whose communications are intercepted, disclosed or used in violation of this provision, and modifies procedures for government interception of communications. Title II creates specific penalties for unlawful access to stored wire and electronic communications, while Title III establishes a general prohibition on the use of pen registers. These titles include specific procedures for access to stored communications and use of pen registers by government entities, and Title II includes a provision for civil actions.

H.R. 4952 requires government entities to compensate private parties assembling or providing information concerning stored electronic communications, or assisting in the installation and use of a pen register. Because such compensation is currently provided in Department of Justice investigations, CBO does not expect these provisions to involve any significant additional cost for the federal government.

Based on information from the Department of Justice, we do not expect enactment of this bill to result in a significant change in the government's law enforcement practices or expenditures. H.R. 4952 would provide a specific foundation in the code for current law enforcement efforts the Department is undertaking under other authority.

If you wish further details on this estimate, we will be pleased to provide them.

With best wishes,

Sincerely,

Rudolph G. Penner, *Director.*

Changes in Existing Law Made by the Bill, as Reported

In compliance with clause 3 of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

PART I—CRIMES

	Sec.
General provisions	1
* * * * * * *	
119. Wire *and electronic communications* interception and interception of oral communications	2510
* * * * * * *	
121. Stored Wire and Electronic Communications and Transactional Records Access	*2701*
* * * * * * *	

CHAPTER 109—SEARCHES AND SEIZURES

* * * * * * *

§ 2232. Destruction or removal of property to prevent seizure

(a) Physical Interference With Search.—Whoever, before, during, or after seizure of any property by any person authorized to make searches and seizures, in order to prevent the seizure or securing of any goods, wares, or merchandise by such person, staves, breaks, throws overboard, destroys, or removes the same, shall be fined not more than $10,000 or imprisoned more than five years, or both.

(b) Notice of Search.—Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise or other property, gives notice or attempts to give notice of the possible search or seizure to any person shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(c) Notice of Certain Electronic Surveillance.—Whoever, having knowledge that a Federal investigative or law enforcement

officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both.

Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years, or both.

* * * * * * *

CHAPTER 119—WIRE *AND ELECTRONIC COMMUNICATIONS* INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Sec.
2510. Definitions.

* * * * * * *

2521. Injunction against illegal interception.

§ 2510. Definitions

As used in this chapter—

(1) "wire communication" means any [communication] *aural transfer* made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception *(including the use of such connection in a switching station)* furnished or operated by any person engaged [as a common carrier] in providing or operating such facilities for the transmission of interstate or foreign communications *or communications affecting interstate or foreign commerce, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;*

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, *but such term does not include any electronic communication;*

* * * * * * *

(4) "intercept" means the aural *or other* acquisition of the contents of any wire, *electronic,* or oral communication through the use of any electronic, mechanical, or other device.

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire [or oral], *oral, or electronic* communication other than—

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a [communications common carrier] *provider of wire or electronic communication service* in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

* * * * * * *

(8) "contents", when used with respect to any wire [or oral], *oral, or electronic* communication, includes any information concerning the [identity of the parties to such communication or the existence,] substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means—

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire [or oral], *oral, or electronic* communications;

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of title 47 of the United States Code; [and]

(11) "aggrieved person" means a person who was a party to any intercepted wire [or oral], *oral, or electronic* communication or a person against whom the interception was directed[.];

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

(B) any wire or oral communication;

(C) any communication made through a tone-only paging device; or

(D) any communication from a tracking device (as defined in section 3117 of this title);

(13) "user" means any person or entity who—

(A) uses an electronic communication service; and

(B) is duly authorized by the provider or such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not—

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

§ 2511. Interception and disclosure of wire or oral communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

(a) willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire [or oral] *oral, or electronic* communication;

(b) willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce, or

(iv) such use or endeavor to use (A) takes place on the permises of any business or other commercial establishment the operations of which affect interstate or foreign

commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) willfully discloses, or endeavors to disclose, to any other person the contents of any wire [or oral] *oral, or electronic* communication, knowing or having reason to know that the information was obtained through the interception of a wire [or oral] *oral, or electronic* communication in violation of this subsection; *or*

(d) willfully uses, or endeavors to use, the contents of any wire [or oral] *oral, or electronic* communication, knowing or having reason to know that the information was obtained through the interception of a wire [or oral] *oral, or electronic* communication in violation of this subsection; [shall be fined not more than $10,000 or imprisoned not more than five years, or both.] *shall be punished as provided in subsection (4).*

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of [any communication common carrier,] *a provider of wire or electronic communication service,* whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property [of the carrier of such communication: *Provided,* That said communication common carriers] *of the provider of that service, except that a provider of wire communication service to the public* shall not utilize service observing or random monitoring except for mechanical or service qualtiy control checks.

(ii) Notwithstanding any other law, *providers of wire or electronic communication service,* [communication common carriers,]their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information facilities, or technical assistance to persons authorized by law to intercept wire [or oral] *, oral, or electronic* communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if [the common carrier,] *such provider* its officers, employees, or agents, landlord, custodian, or other specified person has been provided with—

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No [communication common carrier] *provider of wire or*

electronic communication service officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished an order or certification under this subparagraph, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any violation of this subparagraph by a [communication common carrier] *provider of wire or electronic communication service* or an officer, employee, or agent thereof, shall render the carrier liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any [communication common carrier] *provider of wire or electronic communication service* its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of an order or certification under this subparagraph.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire *or electronic* communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire [or oral], *oral, or electronic* communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire [or oral], *oral, or electronic* communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the pupose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State [or for the purpose of committing any other injurious act].

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an office, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter *or chapter 121,* or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communication [by], *or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing* a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on a frequency assigned to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a common carrier system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled encrypted.

(h) It shall not be unlawful under this chapter—

(i) to use a pen register (as that term is defined for the purpose of chapter 206 (relating to pen registers) of this title);

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service; or

(iii) to use a device that captures the incoming electronic or other impulses which identify the numbers of an instrument from which a wire communication was transmitted.

(3)(A) Except as provided in subparagraph (B) of this paragraph, a person or entity providing an electronic communication service to the public shall not willfully divulge the contents of any communication (other than one to such person or entity, or an agent thereof)

while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(B) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection, whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication, then—

(i) if the communication is not the radio portion of a cellular telephone communication, the offender shall be fined under this title or imprisoned not more than one year, or both; and

(ii) if the communication is the radio portion of a cellular telephone communication, the offender shall be fined not more than $500 or imprisoned not more than six months, or both.

(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of retransmission to the general public is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

§ 2512. Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who willfully—

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication any advertisement of—

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications,

knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined not more than *$10,000* or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for—

(a) [a communications common carrier] *a provider of wire or electronic communication service* or an officer, agent, or employee of, or a person under contract with, [a communications common carrier] *such a provider*, in the normal course of the [communications common carrier's business] *business of providing that wire or electronic communication service*, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a *State*, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications.

§ 2513. Confiscation of wire [or oral], *oral, or electronic* communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be

performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

§ 2515. Prohibition of use as evidence of intercepted wire [or oral], *oral, or electronic* communications

Whenever any wire [or oral], *oral, or electronic* communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

§ 2516. Authorization for interception of wire [or oral], *oral, or electronic* communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, [or] any Assistant Attorney General, *any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division* specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), or chapter 102 (relating to riots);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1084 (transmission of wagering information), *section 751 (relating to escape)*, sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), *section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity),* section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 2252 or 2253 (sexual exploitation of children), sections 2251 and 2252 (sexual exploitation of children), sections [2314] *2312, 2313, 2314,* and 2315 (interstate transportation of stolen property), *the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities),* section 1963 (violations with respect to racketeer influenced and corrupt organizations), *section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud),* or section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassination, kidnapping, and assault);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions); [or]

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain devices) of this title;

(i) the location of any fugitive from justice from an offense described in this section; or

[(h)]*(j)* any conspiracy to commit any of the foregoing offenses.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire [or oral], *oral, or electronic* communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire [or oral], *oral, or electronic* communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or deal-

ing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

§ 2517. Authorization for disclosure and use of intercepted wire [or oral], *oral, or electronic* communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire [or oral], *oral, or electronic* communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire [or oral], *oral, or electronic* communication or evidence derived therefrom any use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire [or oral], *oral, or electronic* communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire [or oral], *oral, or electronic* communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized herein, intercepts wire [or oral], *oral, or electronic* communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

§ 2518. Procedure for interception of wire [or oral], *oral, or electronic* communications

(1) Each application for an order authorizing or approving the interception of a wire [or oral], *oral, or electronic* communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) *except as provided in subsection (11),* a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire [or oral], *oral, or electronic* communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving inteception of wire [or oral], *oral, or electronic* communications within the territorial jurisdiction of the court in which the judge is sitting *(and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction) after within the territorial jurisdiction of the*

court in which the judge is sitting, if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter.

(b) there is probable cause for brief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) *except as provided in subsection (11),* there is probable cause for belief that the facilities from which, or the place where, the wire [or oral], *oral, or electronic* communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire [or oral], *oral, or electronic* communication under this chapter shall specify—

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire [or oral], *oral, or electronic* communication under this chapter shall, upon request of the applicant, direct that a [communication common carrier,] *provider of electronic communication service,* landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such carrier, landlord, custodian, or person is according the person whose communications are to be intercepted. Any communication common carrier, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant [at the prevailing rates] *for reasonable expenses incurred in providing such facilities or assistance.*

(5) No order entered under this section may authorize or approve the interception of any wire [or oral], *oral, or electronic* communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. *Such thirty-day period begins on the earlier of the day on which the*

investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise, subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. *In the event the intercepted communications is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.*

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(a) an emergency situation exists that involves—

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire [or oral], *oral, or electronic* communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire [or oral], *oral, or electronic* communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception

is terminated without an order having been issued, the contents of any wire [or oral], *oral, or electronic* communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)(a) The contents of any wire [or oral], *oral, or electronic* communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire [or oral], *oral, or electronic* communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under this directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire [or oral], *oral, or electronic* communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire [or oral], *oral, or electronic* communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire [or oral], *oral, or electronic* communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

(i) in the case of an application with respect to the interception of an oral communication—

(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General,

the Deputy Attorney General, the Associate Attorney General an Assistant Attorney General, or an acting Assistant Attorney General;

(II) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(III) the judge finds that such specification is not practical; and

(ii) in the case of an application with respect to a wire or electronic communication—

(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(II) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

(III) the judge finds that such purpose has been adequately shown.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order.

§2519. Reports concerning intercepted wire [or oral], *oral, or electronic* communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for *(including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title)*;

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension or an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or

the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire [or oral], *oral, or electronic* communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

§ 2520. Recovery of civil damages authorized

[Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person—

[(a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

[(b) punitive damages; and

[(c) a reasonable attorney's fee and other litigation costs reasonably incurred.

A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or under any other law.]

§ 2520. Recovery of civil damages authorized

(a) In General.—Any person whose wire, oral, or electronic communication is intercepted, disclosed, or willfully used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) Relief.—In an action under this section appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of Damages.—The court may assess as damages in an action under this section whichever is the greater of—

(1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(2) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) Defense.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other provision of law.

(e) Limitation.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

§ 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

§ 2701. Unlawful access to stored communications

(a) Offense.—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communications while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment.—The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—

(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.

(c) Exceptions.—Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703 or 2704 of this title.

§ 2702. Disclosure of contents

(a) Prohibitions.—Except as provided in subsection (b)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity

the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(b) Exceptions.—A person or entity may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2516, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

(6) to a law enforcement agency, if such contents—

(A) were inadvertently obtained by the service provider; and

(B) appear to pertain to the commission of a crime.

§ 2703. Requirements for governmental access

(a) Contents of Electronic Communications in Electronic Storage.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a non-voice wire communication or an electronic communication, that is in electronic storage in an electronic communications system for 180 days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than 180 days by the means available under subsection (b) of this section.

(b) Contents of Electronic Communications in a Remote Computing Service.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscribe or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records Concerning Electronic Communications Service or Remote Computing Service.—A governmental entity may require a provider of electronic communications service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) without required notice to the subscriber or customer if the governmental entity—

(1) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury subpoena;

(2) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

(3) obtains a court order for such disclosure under subsection (d) of this section.

(d) Requirements for Court Order.—A court order for disclosure under subsection (b) or (c) of this section shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State.

§ 2704. Backup preservation

(a) Backup Preservation.—(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subcriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicalbe consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been

made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of—

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than 14 days after the governmental entity's notice to the subscriber or customer if such service provider—

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the government entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determiantion is not subject to challenge by the subscriber or customer or service provider.

(b) Customer Challenges.—(1) Within 14 days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district or State court. Such motion or application shall contain an affidavit or sworn statement—

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer had complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the rea-

sons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or applications decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

§ 2705. Delayed notice

(a) Delay of Notification.—(1) A governmental entity acting under section 2703(b) of this title may—

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed 90 days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed 90 days upon the execution a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse resut for the purposes of paragraph (1) of this subsection is—

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to 90 days each may be granted by the court upon application,

or by certification by a governmental entity, but only in accordance with subsection (b) or (c) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first class mail to, the customer or subscriber a copy of the process or request together with notice that—

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customers or subscriber—

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigtive agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of Notice to Subject of Governmental Access.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

§ 2706. Cost reimbursement

(a) Payment.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such infor-

mation. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) AMOUNT.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

§ 2707. Civil Action

(a) CAUSE OF ACTION.—Any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) RELIEF.—In a civil action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (3); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) DAMAGES.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

(d) DEFENSE.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

§ 2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) DUTY TO PROVIDE.—A Communications common carrier or an electronic communication service provider shall comply with a request made for telephone subscriber information and toll billing information, or electronic communication transactional records made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the carrier or provider to which the request is made that—

(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(c) PROHIBITION OF CERTAIN DISCLOSURE.—No communications common carrier or service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

§ 2710. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.

PART II—CRIMINAL PROCEDURE

CHAPTER 205—SEARCHES AND SEIZURES

§ 3117. Mobile tracking devices

(a) IN GENERAL.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

(b) DEFINITION.—As used in this section, the term "tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or object.

CHAPTER 206—PEN REGISTERS

§ 3121. General prohibition on pen register use; exception

(a) IN GENERAL.—Except as provided in this section, no person may install or use a pen register without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) EXCEPTION.—The prohibition of subsection (a) does not apply with respect to the use of a pen register by a provider of electronic or wire communication service—

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service, or with the consent or the user of that service.

(c) PENALTY.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

§ 3122. Application for an order for a pen register

(a) APPLICATION.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) CONTENTS OF APPLICATION.—An application under subsection (a) of this section shall include—

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

§ 3123. Issuance of an order for a pen register

(a) IN GENERAL.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(b) CONTENTS OF ORDER.—An order issued under this section—

(1) shall specify—

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register is to be attached;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the number and, if known, physical location of the telephone line to which the pen register is to be attached; and

(D) a statement of the offense to which the information likely to be obtained by the pen register relates; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register under section 3124 of this title.

(c) TIME PERIOD AND EXTENSIONS.—(1) An order issued under this section shall authorize the installation and use of a pen register for a period not to exceed 60 days.

(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon

the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed 60 days.

(d) Nondisclosure of Existence of Pen Register.—An order authorizing or approving the installation and use of a pen register shall direct that—

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line to which the pen register is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

§ 3124. Assistance in installation and use of a pen register

(a) In General.—Upon the request of an attorney for the government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

(b) Compensation.—A provider of wire communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

§ 3125. Reports concerning pen registers

The Attorney General shall annually report to Congress on the number of pen register orders applied for by law enforcement agencies of the Department of Justice.

§ 3126. Definitions for chapter

As used in this chapter—

(1) the term "communications common carrier" has the meaning set forth for the term "common carrier" in section 3(h) of the Communications Act of 1934 (47 U.S.C. 153(h));

(2) the term "wire communication" has the meaning set forth for such term in section 2510 of this title;

(3) the term "court of competent jurisdiction" means—

(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register;

(4) the term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted, with respect to wire communications, on the telephone line to which such device is attached, but such term does not include any device used by a provider of wire communication service for billing, or recording as an incident to billing, for communications services provided by such provider; and

(5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

(6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

* * * * * * *

Senate Report Number 99-541

Calendar No. 1064

99TH CONGRESS 2d Session	SENATE	REPORT 99-541

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

OCTOBER 17 (legislative day, OCTOBER 10), 1986.—Ordered to be printed

Mr. THURMOND, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany S. 2575]

The Committee on the Judiciary, to which was referred the bill (S. 2575) having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE

The Electronic Communications Privacy Act amends title III of the Omnibus Crime Control and Safe Streets Act of 1968—the Federal wiretap law—to protect against the unauthorized interception of electronic communications. The bill amends the 1968 law to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.

When the Framers of the Constitution acted to guard against the arbitrary use of Government power to maintain surveillance over citizens, there were limited methods of intrusion into the "houses,

91-010 O

papers, and effects" protected by the fourth amendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions.

The telephone is the most obvious example. Its widespread use made it technologically possible to intercept the communications of citizens without entering homes or other private places. When the issue of Government wiretapping first came before the Supreme Court in *Olmstead* v. *United States*, 277 U.S. 438 (1928), the Court held that wiretapping did not violate the fourth amendment, since there was no searching, no seizure of anything tangible, and no physical trespass.

Today, the *Olmstead* case is often remembered more for Justice Brandeis' prescient dissent than for its holding. Justice Brandeis predicted:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . Can it be that the Constitution affords no protection against such invasions of individual security?

Forty years later, the Supreme Court accepted Justice Brandeis' logic in *Katz* v. *United States*, 389 U.S. 347 (1967), holding that the fourth amendment applies to Government interception of a telephone conversation. At the same time, the Court extended fourth amendment protection to electronic eavesdropping on oral conversations in *Berger* v. *New York*, 388 U.S. 41 (1967).

Congress responded in a comprehensive fashion by authorizing Government interception, under carefully subscribed circumstances in title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510 et seq. Title III is the primary law protecting the security and privacy of business and personal communications in the United States today. Its regimen for protecting the privacy of voice communications is expressly limited to the unauthorized aural interception of wire or oral communications. It only applies where the contents of a communication can be overheard and understood by the human ear. See *United States* v. *New York Telephone Company*, 434 U.S. 159, 167 (1977). Furthermore, existing title III applies only to interceptions of communications sent via common carriers 18 U.S.C. 2510(10).

As Senator Leahy said when he introduced S. 2575 with Senator Mathias, the existing law is "hopelessly out of date." Congressional Record, June 19, 1986. It has not kept pace with the development of communications and computer technology. Nor has it kept pace with changes in the structure of the telecommunications industry.

Today we have large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing.[1] A phone call can be carried by wire, by microwave or fiber optics. It can be transmitted in the form of digitized voice, data or video. Since the divestiture of

[1] These new forms of telecommunications and computer technology are described in the Glossary below.

AT&T and deregulation, many different companies, not just common carriers, offer a wide variety of telephone and other communications services. It does not make sense that a phone call transmitted via common carrier is protected by the current federal wiretap statute, while the same phone call transmitted via a private telephone network such as those used by many major U.S. corporations today, would not be covered by the statute.

These tremendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques. Electronic hardware making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others are readily available in the American market today.

Title I of the Electronic Communications Privacy Act addresses the interception of wire, oral and electronic communications. It amends existing chapter 119 of title 18 to bring it in line with technological developments and changes in the structure of the telecommunications industry.

The Committee also recognizes that computers are used extensively today for the storage and processing of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services. These services as well as the providers of electronic mail create electronic copies of private correspondence for later reference. This information is processed for the benefit of the user but often it is maintained for approximately 3 months to ensure system integrity. For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection. See *United States* v. *Miller*, 425 U.S. 435 (1976) (customer has no standing to contest disclosure of his bank records). Thus, the information may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties. The provider of these services can do little under current law to resist unauthorized access to communications.

Title II of S. 2575 addresses access to stored wire and electronic communications and transactional records. It is modeled after the Right to Financial Privacy Act, 12 U.S.C. 3401 et seq. to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs.

Title III of the bill addresses pen registers and trap and trace devices.

II. History

In 1984, Senator Leahy asked the Attorney General whether he believed interceptions of electronic mail and computer-to-computer communications were covered by the Federal wiretap law. The

Criminal Division of the Justice Department responded that Federal law protects electronic communications against unauthorized acquisition only where a reasonable expectation of privacy exists. Underscoring the need for this legislation, the Department concluded:

> In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as [whether there does or does not exist a reasonable expectation of privacy] are not always clear or obvious.

Senator Leahy's letter and the Justice Department's response mark the beginning of this legislation. The Subcommittee on Patents, Copyrights and Trademarks chaired by Senator Mathias, held hearings in the 98th Congress. See, Hearing before the Subcommittee on Patents, Copyrights and Trademarks of the Committee on the Judiciary on Privacy and Electronic Communications, September 12, 1984, S Hrg. 98-1266

The product of that hearing and subsequent discussions with the Department of Justice and private groups interested in promoting communications privacy, while protecting legitimate law enforcement needs and promoting technological innovation, was S 1667, the Electronic Communications Privacy Act of 1985. Senators Leahy and Mathias introduced that bill on September 19, 1985 On the same day, Congressmen Kastenmeier and Moorhead, the Chairman and Ranking Minority Member of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice introduced an identical bill, H.R. 3378.

In October 1985, the Office of Technology Assessment issued a report entitled "Electronic Surveillance and Civil Liberties." That study concluded that current legal protections for electronic mail are "weak, ambiguous, or non-existent," and that "electronic mail remains legally as well as technically vulnerable to unauthorized surveillance." "Federal Government Information Technology: Electronic Surveillance and Civil Liberties" (Washington, D.C.: U.S. Congress, Office of Technology Assessment, OTA-CIT-293, October 1985).

The Subcommittee on Patents, Copyrights and Trademarks held a hearing on S. 1667 on November 13, 1985. Testimony was received from interested individuals and groups, including representatives of the telephone industry, the electronic mail industry, and the software and service industries. Representatives of the Department of Justice presented their views, and the subcommittee also received testimony from the American Civil Liberties Union and elicited technical information from the Institute of Electrical and Electronics Engineers.

As a result of those hearings, S. 1667 was superseded by a new bill to reflect the concerns raised by some of these groups, particularly the Department of Justice and radio hobbyists On June 19, 1986, Senator Leahy, joined by Senator Mathias, introduced S. 2575.

On August 12, 1986, the Judiciary Committee Subcommittee on Patents, Copyrights and Trademarks favorably reported S. 2575, as amended, to the full Committee by voice vote.

On September 19, 1986, Senators Leahy and Mathias and Chairman Thurmond offered an amendment in the nature of a substitute to S. 2575. The Committee voted unanimously to favorably report the Electronic Communications Privacy Act of 1986, as amended, to the full Senate.

III. Statement

A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations. Voice communications transmitted via common carrier are protected by title III of the Omnibus Crime Control and Safe Streets Act of 1968.

But there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology. This is so, even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services.

This gap results in legal uncertainty. It may unnecessarily discourage potential customers from using innovative communications systems. It probably encourages unauthorized users to obtain access to communications to which they are not a party. It may discourage American businesses from developing new innovative forms of telecommunications and computer technology. The lack of clear standards may expose law enforcement officers to liability and may endanger the admissibility of evidence.

Most importantly, the law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

The Committee believes that S. 2575, te Electronic Communications Privacy Act of 1986, represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies.

The Justice Department strongly supports S. 2575 because it strengthens the current wiretap law from a law enforcement perspective Specifically, it expands the list of felonies for which a voice wiretap order may be issued and the list of Justice Department officials who may apply for a court order to place a wiretap. The bill also includes provisions making it easier for law enforcement officials to deal with a target who repeatedly changes telephones to thwart interception of his communications and creates criminal penalties for those who notify a target of a wiretap in order to obstruct it. These provisions will be particularly helpful to the Justice Department in its fight against drug trafficking.

The organizations and individual corporations named below also support the principles embodied in the legislation.

Organizations: Electronic Mail Assoc.; ADAPSO; Telocator Network of America; Cellular Telecommunications Industry Assoc.;

ACLU; National Association of Manufacturers (NAM); U.S. Chamber of Commerce; National Association of Broadcasters (NAB); National Cable Television Assoc. (NCTA); National Association of Business & Educational Radio (NABER); CBEMA; U.S. Telephone Assoc.; Videotext Industry Assoc.; Information Industry Assoc.; Electronic Funds Transfer Assoc.; Radio and Television News Directors Assoc.; Association of American Railroads; Institute of Electrical and Electronics Engineers (IEEE); Direct Marketing Association; Utilities Telecommunications Council; and Associated Credit Bureaus, Inc.

Corporations: AT&T; General Electric; IBM; GTE; EDS; ITT; MCI; CBS; ABC; NBC; Tandy Corp. (Radio Shack); Trintex; Equifax; TRW; Source Telecomputing Corporation; Chase Manhattan Bank; Motorola; Ameritech; Bell Atlantic; Bell South; Southwestern Bell; NYNEX; Pacific Telesis; US West; and Associated Credit Services, Inc.

A few points in the development of the Electronic Communications Privacy Act of 1986 should be noted here. After Senators Leahy and Mathias introduced the bill in June 1986, S. 2575 was referred to the Subcommittee on Patents, Copyrights and Trademarks. During the subcommittee markup session held on August 12, 1986, the bill was further amended to clarify certain provisions.

At the request of the FCC, in response to the recent Captain Midnight incident, in which an individual in Florida interfered with the transmission of an HBO program being relayed by satellite, the subcommittee included in the bill language to address deliberate or malicious interference with satellite transmissions. It also added to title III of the bill related to installation and use of pen registers, procedural requirements for orders to use "trap and trace" devices.

In order to underscore that the inadvertent reception of a protected communication is not a crime, the subcommittee changed the state of mind requirement under title III of the Omnibus Crime Control and Safe Streets Act of 1968 from "willful" to "intentional." This change in the law addresses the concerns of radio scanners that in the course of scanning radio frequencies in order to receive public communications, one could inadvertently tune through a protected communication like a cellular telephone call. This provision makes clear that the inadvertent interception of a protected communication is not unlawful under this Act.

During subcommittee consideration, Senators Laxalt, Grassley, DeConcini and Simpson expressed concerns about the bill's penalty structure for the interception of certain satellite transmissions by home viewers. Senators Leahy and Mathias agreed that those concerns would be addressed during Committee consideration of the Electronic Communications Privacy Act.

The Leahy-Mathias-Thurmond substitute for S. 2575, which was offered when the full Committee considered this legislation, incorporated an amendment offered by Senator Grassley. Senators Laxalt, McConnell, Simpson and Denton cosponsored Senator Grassley's amendment.

Senator Grassley's amendment modifies the criminal penalties and civil liability provisions of chapter 119 of title 18 of the United States Code so that there is a two-track, tiered penalty structure for home viewing of private satellite transmissions when the con-

duct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain.

In a public action, under the Grassley amendment, a first offender would be subject to a suit by the Government for injunctive relief. If injunctive relief is granted, one who violates the injunction would be subject to the full panoply of enforcement mechanisms within the court's existing authority, including criminal and civil contempt. Second and subsequent offenses carry a mandatory $50 civil fine for each violation. The term "violation" in this context refers to each viewing of a private video communication.

In a private civil action, a person harmed by the private viewing of such a satellite communication may sue for damages. If the defendant has not previously been enjoined in a government action as described above, and has not previously been found liable in a civil suit, the plaintiff may recover the greater of his actual damages or statutory damages of $50 to $500. A second offender (one who has been found liable in a prior private civil action or one who has been enjoined in a government suit) is subject to liability for the greater of actual damages or statutory damages of $100 to $1,000. Third and subsequent offenders are subject to the bill's full civil penalties.

The Grassley amendment also takes outside the penalty provisions of the Electronic Communications Privacy Act, the interception of a satellite transmission via audio subcarrier if the transmission is intended for redistribution to facilities open to the public, provided that the conduct is not for the purpose of direct or indirect commercial advantage or private financial gain. Audio subcarriers intended for redistribution to the public include those for redistribution by broadcast stations and cable and like facilities. They also include those for redistributions to buildings open to the public like hospitals and office buildings that pump in music which has been transmitted via subcarrier. As specified in the substitute, this audio subcarrier exclusion does not apply to data transmissions or telephone calls.

The substitute amendment also incorporated Senator Simon's amendment. Senator Simon had expressed concern that the Electronic Communications Privacy Act's penalties were too severe for the first offender, who without an unlawful or financial purpose, intercepts a cellular telephone call or certain radio communications related to news-gathering.

Senator Simon's amendment reduces the penalty for such an interception of an unencrypted, unscrambled cellular telephone call to a $500 criminal fine. Unencrypted, unscrambled radio communications transmitted on frequencies allocated under subpart D of part 74 of the FCC rules are treated like private satellite video communications are under Senator Grassley's amendment.

Scanning enthusiasts have argued to the Committee that the mere monitoring of cellular telephone calls should not be illegal. That argument ignores three important realities. First, Congress, in passing the 1968 wiretap law already made willful monitoring of such telephone calls illegal when at least part of the conversation is carried by wire. Second, unlike many signals which are more commonly scanned, the design of the cellular telepnone system makes the intentional monitoring of specific calls more difficult be-

cause they are handed off among cells. The Committee is not convinced that these arguments overcome the need for protection of privacy interests.

It has been suggested that the Federal Communications Commission consider labeling requirements on cellular telephnones, radio scanning equipment and private satellite video communications. The Commission might consider the feasibility of requiring that cellular telephones be labeled to indicate that cellular calls are radio-based communications, and as such, portions of the communication may be intercepted by available scanning equipment and of requiring that scanning equipment be labeled to indicate that the intentional interception of protected communications could be a Federal criminal violation. Finally, the Commission might consider the feasibility of requiring those who transmit private satellite video communications to periodically transmit a crawl across the bottom of the screen indicating that such communications are protected.

IV. Glossary

For reference, some of the new telecommunications and computer technologies referred to in the Electronic Communications Privacy Act of 1986 and this report are described briefly below. Treatment of these and other technologies under current law is discussed in the House Report to its companion measure, H.R. 4952. *See* House Report 99–647.

Electronic Mail

Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines. In its most common form, messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer "mail box" until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer. If the addressee is not a subscriber to the service, the electronic mail company can put the message onto paper and then deposit it in the normal postal system.

Electronic mail systems may be available for public use or may be proprietary, such as systems operated by private companies for internal correspondence.

Computer-to-Computer Communications

Common computer-to-computer communications include the transmission of financial records or funds transfers among financial institutions, medical records between hospitals and/or physicians' offices, and the transmission of proprietary data among the various offices of a company.

Electronic Bulletin Boards

Electronic "bulletin boards" are communications networks created by computer users for the transfer of information among com-

puters. These may take the form of proprietary systems or they may be noncommercial systems operating among computer users who share special interests. These noncommercial systems may involve fees covering operating costs and may require special "passwords" which restrict entry to the system. These bulletin boards may be public or semi-public in nature, depending on the degree of privacy sought by users, operators or organizers of such systems.

Microwave

Microwave consists of extremely high frequency radio waves transmitted point-to-point on line-of-sight paths between antennas located on towers or building tops (in terrestrial microwave systems) and between satellites and earth station "dish" antennas (in satellite-based systems).

Cellular Telephones

In 1981 the Federal Communications Commission approved the use of cellular telephone services. This technology uses both radio transmission and wire to make "portable" telephone service available in a car, a briefcase, or in rural areas not reached by telephone wire.

In a cellular radiotelephone system, large service areas are divided into honeycomb-shaped segments or "cells"—each of which is equipped with a low-power transmitter or base station which can receive and radiate messages within its parameters. When a caller dials a number on a cellular telephone, a transceiver sends signals over the air on a radio frequency to a cell site. From there the signal travels over phone lines or a microwave to a computerized mobile telephone switching office ("MTSO") or station. The MTSO automatically and inaudibly switches the conversation from one base station and one frequency to another as the portable telephone, typically in a motor vehicle, moves from cell to cell.

Cellular technology, because it is more complex, is more difficult to intercept than traditional mobile telephones; it is, however, more accessible than microwave transmissions. Cellular telephone calls can be intercepted by either sophisticated scanners designed for that purpose, or by regular radio scanners modified to intercept cellular calls.

Cordless Telephones

A cordless telephone consists of a handset and a base unit wired to a landline and a household/business electrical current. A communication is transmitted from the handset to the base unit by AM or FM radio signals. From the base unit the communication is transmitted over wire, the same as a regular telephone call. The radio portions of these telephone calls can be intercepted with relative ease using standard AM radios.

Electronic Pagers

Electronic pagers are radio activated devises through which a user is notified of another's attempt to contact the carrier of the portable paging unit. These are in wide use among persons who are away from their homes or offices—or, more precisely, away from telephones or two-way radios—yet still need to be reachable by others.

Pagers take on one of three basic forms: "tone only," "display" and "tone and voice pagers." The "tone only" device emits a "beep" or other signal to inform the user that a message is waiting, and where that message can be retrieved by the user's making a phone call to a predetermined number (usually an office or answering service). "Display" pagers are equipped with screens that can display visual messages, usually the telephone number of the person seeking to reach the person being paged. The party seeking to make contact with the user is instructed to provide a message, usually by pushing the buttons of a touch-tone telephone; this message is stored by the paging company's computer until it can be transmitted to the user's pager, where the message can then be read directly by the user, obviating the need for the user to make a telephone call to retrieve the message. The most sophisticated type of pager is the "tone and voice" model. It can receive a spoken message that the paging company's computer has taken from the party seeking to contact the unit's user. After the beep tone is made, the device "repeats" the recorded message. This requires that a radio signal containing voice communications be sent from the paging company's base to the mobile unit.

PEN REGISTERS/TRAP AND TRACE DEVICES

Pen registers are devices that record the telephone numbers to which calls have been placed from a particular telephone. These capture no part of an actual telephone conversation, but merely the electronic switching signals that connect two telephones. The same holds true for trap and trace devices, which record the numbers of telephones from which calls have been placed to a particular telephone.

ELECTRONIC TRACKING DEVICES (TRANSPONDERS)

These are one-way radio communication devices that emit a signal on a specific radio frequency. This signal can be received by special tracking equipment, and allows the user to trace the geographical location of the transponder. Such "homing" devices are used by law enforcement personnel to keep track of the physical whereabouts of the sending unit, which might be placed in an automobile, on a person, or in some other item.

REMOTE COMPUTER SERVICES

In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data in-house on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today businesses of all sizes—hospitals, banks and many others—use remote computing services for computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information

supplied by the subscriber or customer. Data is most often transmitted between these services and their customers by means of electronic communications.

V. SECTION-BY-SECTION ANALYSIS

Section 1 provides that the short title of the bill is the "Electronic Communications Privacy Act of 1986."

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

Under current law, the interception of wire and oral communications are governed by chapter 119 of title 18 (18 U.S.C. 2510 et seq.) Title I of the Electronic Communications Privacy Act expands chapter 119 to take into account modern advances in electronic telecommunications and computer technology.

Section 101—Federal penalties for the interception of communications

Definitions for terms used in chapter 119 and new chapter 121 of title 18 are set out in section 101 of the bill. This section also describes conduct which is not unlawful under this Act and modifies the penalties set out in existing section 2511 of title 18. It provides that the remedies in chapter 119 are the exclusive statutory remedies for violations of this chapter. Technical amendments to chapter 119 are also included in Section 101 of the bill.

Subsection 101(a)—Definitions

Subsection 101(a) of the Electronic Communications Privacy Act sets out the definitions and amendments to definitions used in chapter 119 and new chapter 121 of title 18. Paragraph 101(a)(1) amends the definition of the term "wire communication" in subsection 2510(1) of title 18.

Subparagraph (A) amends that definition to include aural transfers. As defined in proposed subsection 2510(18) of title 18, "aural transfers" are those which include the human voice at any point between and including the points of origin and reception.

Subparagraph (B) specifies that the use of wire, cable or other similar connections for the transmission of communications includes the use of such connections in a switching station. This subparagraph makes clear that cellular communications—whether they are between two cellular telephones or between a cellular telephone and a "land line" telephone—are included in the definition of "wire communications" and are covered by the statute. As noted below, the bill distinguishes between cordless and cellular telephones.

Recognizing that since deregulation and the divestiture of AT&T, many different companies, not just common carriers, offer and use telephone and other communications services, subpargraph (C) deletes from the definition of "wire communication" the requirement that communications must be transmitted via common carrier to be covered by the federal wiretap statute.

Subparagraph (D) specifies that wire, cable or similar connections furnished or operated by any person engaged in providing or operating such facilities for the transmission of "communications

affecting interstate or foreign commerce," are within the definition of a "wire communication." This language recognizes that private networks and intra-company communications systems are common today and brings them within the protection of the statute. However, that language is not meant to suggest that the Electronic Communications Privacy Act applies to interceptions made outside the territorial United States. Like the Omnibus Crime Control and Safe Streets Act of 1968 which it revises, the Electronic Communications Privacy Act regulates only those interceptions conducted within the territorial United States.

The Senate Judiciary Committee's Subcommittee on Patents, Copyrights and Trademarks amended subparagraph (D) to specify that wire communications in storage like voice mail, remain wire communications, and are protected accordingly.

The combined effect of subparagraphs (A) through (D) is to clarify that the term "wire communication" means the transfer of a communication which includes the human voice at some point. The transfer must be made in whole or in part through the use of communication transmission facilities by the aid of wire, cable, or other like connection, including fiber optics. The facilities may be furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or he may provide or operate those facilities for the transmission of communications affecting interstate or foreign commerce.

Thus, a wire communication encompasses the whole of a voice telephone transmission even if part of the transmission is carried by fiber optic cable or by radio—as in the case of cellular telephones and long distance satellite or micowave facilities. The conversion of a voice signal to digital form for purposes of transmission does not render the communication non-wire. The term "wire communication" includes existing telephone service, and digitized communications to the extent that they contain the human voice at the point of origin, reception, or some point in between. A private telephone system established by a company whose activities affect interstate commerce, would also be covered.

It should be noted that an improperly mechanical reading of the phrase "in whole or in part * * * by the aid of wire * * *" could sweep in virtually all voice communications made with the aid of any electronic equipment, inasmuch as virtually all such equipment includes in its assembly some length of wire or the equivalent. The quoted is intended to refer to wire that carries the communication to a significant extent from the point of origin to the point of reception, even in the same building. It does not refer to wire that is found inside the terminal equipment at either end of the communication.

Subparagraph (D) specifies that the term "wire communication" does not include the radio portion of a cordless telephone communication transmitted between the cordless handset and the base unit. Because communications made on some cordless telephones can be intercepted easily with readily available technologies, such as an AM radio, it would be inappropriate to make the interception of such a communication a criminal offense. The wire portion of a cordless communication remains fully covered, however.

Section 101(a)(2) of the Electronic Communications Privacy Act amends the definition of "oral communication" in current section 2510(2) of title 18 to exclude electronic communications. There have been cases involving radio communications in which the court having determined that the radio communication was not a wire communication then analyzes it in privacy terms to determine if it is an oral communication. The bill rejects that analysis by excluding electronic communications from the definition of oral communications.

An oral communication is an utterance by a person under circumstances exhibiting an expectation that the communication is not subject to interception, under circumstances justifying such an expectation. In essence, an oral communication is one carried by sound waves, not by an electronic medium.

Section 101(a)(3) of the Electronic Communications Privacy Act amends the definition of the term "intercept" in current section 2510(4) of title 18 to cover electronic communications. The definition of "intercept" under current law is retained with respect to wire and oral communications except that the term "or other" is inserted after "aural." This amendment clarifies that it is illegal to intercept the non-voice portion of a wire communication. For example, it is illegal to intercept the data or digitized portion of a voice communication.

Subsection 101(a)(4) of the Electronic Communications Privacy Act amends existing section 2510(5) of title 18 to clarify that telephone equipment provided by the user and connected to the facilities of a service provider is not an "electronic, mechanical or other device," provided that it is used in the ordinary course of the user's business.

The Committee notes that proposed section 2510's definition of an "electronic, mechanical or other device" includes any combination of parts designed or intended for use in converting those parts into such a device or apparatus and from which such a device or apparatus may be readily assembled. The Committee also notes that section 2512, as amended by the Electronic Communications Privacy Act, prohibits the manufacture, distribution, possession, and advertising only of devices primarily useful for surreptitious interception.

Subsection 101(a)(5) of the Electronic Communications Privacy Act amends current section 2510(8) of title 18 to exclude from the definition of the term "contents," the identity of the parties or the existence of the communication. It thus distinguishes between the substance, purport or meaning of the communication and the existence of the communication or transactional records about it.

The Supreme Court has clearly indicated that the use of pen registers does not violate either chapter 119 of title 18 or the fourth amendment. Subsection 101(a)(5) of this legislation makes that policy clear. It should be read in conjunction with Title III of the Electronic Communications Privacy Act which adds new chapter 206 on pen registers and trap and trace devices to title 18. Subsection 101(a)(5) of the bill does not affect the installation or use of pen registers under the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1801 et. seq. Similarly, the omission of a conforming amendment to the definition of "contents" in section 705 of title 47 is not intended to affect the current law under that section with respect to pen registers. The use of pen registers has been found not to violate section 705. See *Hodge* v. *Mountain States Tel. & Telegraph Co.*, 555 F.2d 254 (9th Cir. 1977).

Subsection 101(a)(6) of the Electronic Communications Privacy Act adds to section 2510 of title 18 definitions for the terms "electronic communication," "electronic communications system," "electronic communication service," "readily accessible to the general public," "electronic storage," and "aural transfer."

An "electronic communication" is defined in proposed subsection 2510(12) of title 18 as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or a photooptical system that affects foreign or interstate commerce." The following are explicitly excluded from the definition: (A) the radio portion of a cordless telephone communication transmitted between the cordless phone handset and the base unit; (B) any wire or oral communication; (C) any communication made through a tone-only paging device; (D) any communication from a tracking device.

As a general rule, a communication is an electronic communication protected by the federal wiretap law if it is not carried by sound waves and cannot fairly be characterized as containing the human voice. Communications consisting solely of data, for example, and all communications transmitted only by radio are electronic communications. This term also includes electronic mail, digitized transmissions, and video teleconferences. Although radio communications are within the scope of the Act, the provisions of the Electronic Communications Privacy Act directed specifically to radio do not affect the applicability of section 705 of the Communications Act of 1934, as amended, to actions by members of the public.

Under proposed subsection 2510(13), the term "user" is defined as any person or entity who (A) uses an electronic communication service and (B) is duly authorized by the service provider to do so.

An "electronic communication system" is defined in proposed subsection 2510(14). Such a system encompasses any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications as well as any computer facilities or related electronic equipment for the electronic storage of such communications.

An "electronic communication service" is defined in proposed subsection 2510(15) of title 18 as a service which provides its users the ability to send or to receive wire or electronic communications. Such services can be provided through the same facilities. Existing telephone companies and electronic mail companies are providers of electronic communication services. Other services like remote computing services may also provide electronic communication services.

Radio communications "readily accessible to the general public" are defined in proposed subsection 2510(16). Radio communications are considered readily accessible to the general public unless they fit into one of five specified categories.

As described below, subsection 101(b) of the Electronic Communications Privacy Act provides an exception to the general prohibitions on interception for electronic communications which are configured to be readily accessible to the general public. Thus, the radio communications specified in proposed subsection 2510(16) are afforded privacy protections under this legislation unless another exception applies.

As specified in paragraph (A) of proposed subsection 2510(16), scrambled or encrypted radio communications are not readily accessible to the general public. The terms are used in their technical sense. To "encrypt" or to "scramble" means to convert the signal into unintelligible form by means intended to protect the contents of a communication from unintended recipients. Methods which merely change the form of a plaintext message, e.g., a device which converts an analog signal to a digital stream, does not provide "encryption" within the meaning of this bill. Nor does the use of a word code, no matter how sophisticated, amount to scrambling or encryption. Examples of scrambling techniques which are currently available include the data encryption standard (DES).

As specified in paragraph (B) radio communications transmitted through modulation techniques whose essential parameters have been withheld from the public in order to preserve the privacy of the communication are not readily accessible to the general public. This paragraph (B) refers to spread spectrum radio communications. Spread spectrum technology usually involves the transmission of a signal on different frequencies where the receiving station must possess the necessary algorythm in order to reassemble the signal.

As specified in paragraph (C) of proposed subsection 2510(16) of title 18, radio communications carried on a subcarrier or other signal subsidiary to a radio transmission are protected by the Electronic Communications Privacy Act. This category includes, for example, data and background music services carried on FM subcarriers. It also includes data carried on the Vertical Blanking Interval (VBI) of a television signal.

Radio communications transmitted over a system provided by a common carrier are not readily accessible to the general public with one exception. That exception is for tone-only paging systems. As a result of that exception, the interception of tone-only paging system transmissions will not be prohibited by this law. However, the unauthorized interception of a display paging system, which invovles the transmission of alphanumeric characters over the radio, carried by a common carrier, is illegal.

As specified in proposed paragraph (E), radio communications transmitted on frequencies allocated under parts 25 and 94 and subparts D, E, an F of part 74 of the FCC rules are protected by the Electronic Communications Privacy Act. These communications include satellite communications, auxiliary broadcast services and private microwave services, each of which routinely carries private business or personal communications. Two-way voice radio communications made on frequencies shared with services outside part 74 are expressly excluded from this category of protected communications.

The liability incurred under chapter 119 for the interception of the communications described in proposed paragraph 2510(16)(E) may be limited. Section 101(b) of the Electronic Communications Privacy Act sets out exceptions from liability under this Act with respect to electronic communications and section 101(d) establishes the penalty structure for violations of this Act.

The term "electronic storage" is defined in proposed subsection 2510(17) of title 18. Electronic storage means (A) the temporary, intermediate storage of a wire or electronic communication incidental to its transmission as well as (B) the storage of such communication by an electronic communications service for backup protection. The term covers storage within the random access memory of a computer as well as storage in any other form including storage of magnetic tapes, disks or other media. Thus, for example, section 2701's prohibitions against unauthorized access to wire or electronic communications while they are in electronic storage would prohibit unauthorized access to such a communication while it is stored on magnetic tape or disk. The section 2701 prohibitions similarly would apply to information held on magnetic tape or disk pursuant to an agreement to provide remote computing services.

The last new definition in subsection 101(a)(6) of the Electronic Communications Privacy Act is the definition of an "aural transfer" in proposed subsection 2510(18). An aural transfer means any transfer containing the human voice at any point between and including the points of origin and reception. Under this definition, voice messages transferred over a paging system are protected. It is intended that computer-generated or otherwise artificial voices are not included in this definition and thus will not be part of a "wire communication." They would, however, be part of an "electronic communication."

It is important to recognize that a transaction may consist, in part, of both electronic communications and wire or oral communications as those terms are defined in section 2510 of title 18, as amended by the Electronic Communications Privacy Act. Accordingly, different aspects of the same communication might be characterized differently. For example, the transmission of data over the telephone is an electronic communication. If the parties use the line to speak to one another between data transmissions, those communications would be wire communications. At the same time, for a person overhearing one end of the telephone conversation by listening in on the oral utterances of one of the parties, those utterances are oral communications.

Although this bill does not address questions of the application of title III standards to video surveillance and only deals with the interception of closed circuit television communications to a limited extent, closed circuit television communications do provide another example of the importance of, and the interrelationship between, the definitions contained in this legislation. If a person or entity transmits a closed circuit television picture of a meeting using wires, microwaves or another method of transmission, the transmission itself would be an electronic communication. Interception of the picture at any point without either consent or a court order would be a violation of the statute. By contrast, if law enforcement officials were to install their own cameras and create their own

closed circuit television picture of a meeting, the capturing of the video images would not be an interception under the statute because there would be no interception of the contents of an electronic communication. Intercepting the audio portion of the meeting would be an interception of an oral communication, and the statute would apply to that portion.

Section 101(b)—Exceptions with respect to electronic communications

Subsection 2511(1) of title 18 of the United States Code sets out prohibitions against the interception, disclosure and use of wire or oral communications. Subsection 2511(2) specifies conduct which is not unlawful under chapter 119 of title 18.

Subsection 101(b) of the Electronic Communications Privacy Act amends Subsection 2511(2). Paragraph 101(b), consistent with other provisions of this legislation, deletes references to common carriers. It thus clarifies that any service provider who discloses the existence of an interception or surveillance or the device used to accomplish the interception or surveillance would be liable for civil damages under Section 2520 of title 18.

Paragraph 101(b)(2) of the Electronic Communications Privacy Act amends section 2511(2)(d) of title 18 by striking out "or for the purpose of committing any other injurious act". Under current Federal law it is permissible for one party to consent to the interception of a conversation unless that interception is for illegal, tortious or other injurious purposes such as blackmail. In numerous court cases the term "other injurious purposes" has been misconstrued. Most troubling of these cases have been attempts by parties to chill the exercise of first amendment rights through the use of civil remedies under this chapter. For example, in *Boddie* v. *American Broadcasting Co.*, 731 F.2d 333 (6th Cir. 1984), the plaintiff, whose conversations were recorded by a journalist, sued. Despite the consent of the reporter who was a party to the conversation, the plaintiff claimed that the recording of the conversation was illegal because it was done for an improper purpose, to embarrass her. While the appeals court decision in *Boddie* merely sent the case back for further factual development, it is clear from the facts of the case that the term "improper purpose" is overly broad and vague. The court's opinion suggests that if the network intended to cause "insult and injury" to plaintiff Boddie, she might be entitled to recover. This interpretation of the statute places a stumbling block in the path of even the most scrupulous journalist. Many news stories have been brought to light by recording a conversation with the consent of only one of the parties involved—often the journalist himself. Many news stories are embarrassing to someone. The present wording of section 2511(2)(d) not only provides such a person with a right to bring suit, but it also makes the actions of the journalist a potential criminal offense under section 2511, even if the interception was made in the ordinary course of responsible news-gathering activities and not for the purpose of committing a criminal act or a tort. Such a threat is inconsistent with the guarantees of the first amendment. Inasmuch as chapter 119 as amended by the Electronic Communications Privacy Act continues to prohibit interceptions made for the purpose of committing either a crime or a tort (including defamation), the public will be afforded ample portection against improper or unscrupulous interception.

Subsection 101(b)(3) of the Electronic Communications Privacy Act amends section 2511(2)(f) of title 18 to clarify that nothing in chapter 119 as amended or in proposed chapter 121 affects existing legal authority for U.S. Government foreign intelligence activities involving foreign electronic communications systems. The provision neither enhances nor diminishes existing authority for such activities; it simply preserves the status quo. It does not provide authority for the conduct of any intelligence activity.

Further the Senate expects that the practice of providing to the House and Senate Intelligence Committees proposed changes in relevant executive branch procedures and regulations governing the conduct of intelligence activities, including those involving electronic surveillance, physical searches, and the minimization of information collected concerning U.S. persons will be continued. As in the past, the Senate expects that any relevant changes in these procedures and regulations will be provided to the Senate and House Intelligence Committees prior to their taking effect.

Finally, since Congress last addressed the issue of privacy communications in a comprehensive fashion, the technologies of communication and interception have changed dramatically, and are expected to continue to do so. These factors have raised serious issues about the protection of the privacy interests of U.S. citizens, which are of great concern to the Senate and to the American people. For this reason, the Senate wishes to emphasize the obligation of the heads of intelligence agencies to continue to keep the Select Committee on Intelligence fully and currently informed of all intelligence activities pursuant to title V of the National Security Act of 1947.

Subsection 101(b)(4) of the Electronic Communications Privacy Act amends section 2511(2)(g) of title 18 of the United States Code. It sets out new exemptions from criminal liability applicable to the technologies which this legislation adds to the privacy protections of the federal wiretap law. Proposed section 2511(2)(g) provides that it shall not be unlawful under chapters 119 or 121 of title 18 for any person to engage in the conduct described in its five subparagraphs.

Under proposed section 2311(2)(g)(i), it is permissible to intercept electronic communications made through an electronic communication system configured so that the conmmunication is "readily accessible to the general public." That term is defined with respect to radio communications in proposed section 2510(16) of title 18. The term "configure" is intended to establish an objective standard of design configuration for determining whether a system receives privacy protection.

Under this provision, it would not be unlawful to intercept subcarrier and UBI communications that are transmitted for the use of the general public. Such "public" communications would include the stereo subcarrier used in FM broadcasting or data carried on the VBI to provide closed-captioning of TV programming for the hearing-impaired.

Under proposed section 2511(g)(ii) it is permissible to intercept any radio communication which is transmitted (I) by any station

for the use of the general public, or that relate to ships, aircraft, vehicles or persons in distress; (II) by any government, law enforcement, civil defense, private land mobile or public safety communications system (including police and fire), that is readily accessible to the general public; (III) by a station operating on an authorized frequency within the bands allocated to amateur, citizens band or general mobile radio services; or (IV) by any marine or aeronautical communications system.

Traditionally, these radio communications have been free from prohibitions on mere interception. Amateur radio communications, including those utilizing telephone interconnect or amateur radio computer linked message systems are certainly not those to which this legislation is aimed. All amateur radio communications conducted on radio frequencies allocated to the Amateur Radio Services are exempt from this bill's prohibitions against the interception of electronic communications.

Radio services readily accessible to the general public are exempt from this act's prohibitions against interception by the generic exception contained in proposed paragraph 2511(2)(g)(i).

Proposed section 1511(2)(g)(iii) addresses conduct which is either prohibited or permitted by the Communications Act of 1934, as amended. Under clause (I) of subparagraph (iii) it is not unlawful under chapter 119 or 121 of title 18 for any person to engage in conduct prohibited by section 633 of the Communications Act of 1934 relating to cable piracy. If an individual violates the criminal prohibitions in section 633 of the Communications Act, he cannot also be charged under chapters 119 or 121 of title 18.

Clause (II) exempts from the prohibitions on interception contained in this Act conduct which is excepted from section 705(a) of the Communications Act by virtue of section 705(b) of that Act. Thus, if conduct is permitted under section 705(b) of the Communications Act, engaging in that conduct would not be a crime under chapters 119 or 121 of title 18, as amended by the Electronic Communications Privacy Act. Determination of whether conduct is permitted under section 705(b) must, of course, be the result of an examination of the statute, relevant legislative history, existing court interpretations and constructions given the statute by appropriate federal regulatory entities.

Proposed section 2511(2)(g)(iv) of title 18 exempts from the criminal prohibition contained in chapters 119 and 121 of that title, the interception of any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of such interference.

Finally, proposed section 2511(2)(g)(v) exempts interceptions of radio communication by other users of the same frequency when such communication is made through a system that utilizes frequencies monitored by individuals engaged in the provision or use of such a system. This exemption clarifies that it is not unlawful for users of the same frequency, who must listen to be sure a channel is clear before using it, to do so. The exception applies to users of common and non-common carrier systems, but does not apply if the communication is scrambled or encrypted.

Subsection 101(b)(4) of the Electronic Communications Privacy Act amends subsection 2511(2) of title 18 to add a new paragraph (h) to that subsection. Proposed subparagraph (i) of paragraph (h) clarifies that the use of pen registers and trap and trace devices are not regulated by chapter 119 of title 18. The use of those devices will be regulated by new chapter 206 of title 18 as amended by the Electronic Communications Privacy Act.

Subparagraph (ii) of paragraph (h) states that no violation of this chapter occurs if a provider of wire or electronic communication service records the fact that a communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication or a user of that service, from fraudulent, unlawful or abusive use of such a service. This provision permits the electronic and wire communication providers to protect themselves and their customers.

Subsection 101(c)—Technical and conforming amendments

Subsection (c) sets out technical and conforming amendments to chapter 119 of title 18. Paragraph (c)(1) adds "electronic communication" in appropriate places throughout the chapter. Paragraph (c)(2) amends the heading of the chapter. Paragraph (c)(3) amends the table of chapters to add electronic communications to the table. Paragraphs (4), (5), (6), (7), and (8) of subsection 101(c) of the Electronic Communications Privacy Act make appropriate technical amendments to delete the term "common carrier" and substitute in its place "provider of wire or electronic communication."

Section 2511(2)(a)(i), as amended, specifies that it is not unlawful for the employees of providers of wire or electronic communication services to intercept, disclose or use customer communications in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of the service or to the protection of the rights or property of the provider, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality checks.

In applying the second clause only to wire communications, this provision reflects an important technical distinction between electronic communications and traditional voice telephone service. The provider of electronic communications services may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain. These monitoring functions, which may be necessary to the provision of an electronic communication service, do not involve humans listening in on voice conversations. Accordingly, they are not prohibited. In contrast, the traditional limits on service "observing" and random "monitoring" do refer to human aural interceptions and are retained with respect to voice or "wire" communications.

Subsection 101(d)—Penalties modification

Subsection 101(d) of the Electronic Communications Privacy Act modifies the general penalty structure for violations of this chapter. It sets out proposed subsections (4) and (5) of section 2511 of title 18. Subsection (4) sets out the criminal penalties for violations

of subsection 2511(1). Subsection (5) outlines the injunctive relief available to the federal government in the case of specified conduct related to private satellite video communications that are not scrambled or encrypted and to communications transmitted on frequencies allocated under subpart D of part 74 of the FCC rules that are not scrambled or encrypted.

The general rule as set out in proposed paragraph 2511(4)(a) is that a violation is punishable as a 5-year felony. Unless one of the exceptions in proposed subsection 2511(4)(b) or subsection 2511(5) applies, a person violating section 2511(1) will be liable for a fine under this chapter, imprisonment up to 5 years, or both. The fines under the chapter are set by section 3623 of title 18. That section provides for a different maximum fine level for felonies or misdemeanors resulting in death. Individual defendants can be fined up to $250,000 and organizations can be fined up to $500,000.

As stated in proposed paragraph 2511(14)(b), the first exception to the general rule that violations are 5-year felonies, applies to unscrambled, unencrypted radio communications provided that the conduct is a first offense and is not for a tortious or illegal purpose or purposes of direct or indirect commerical advantage or private financial gain. If the radio communication is scrambled or encrypted, if the person violating the statute has been found guilty of a prior offense, or if his conduct was for one of the enumerated bad purposes, the conduct remains punishable as a 5-year felony.

As stated in subparagraph (ii) of proposed paragraph 2511(4)(b), for first offenders whose conduct was not for one of the enumerated bad purposes, if the communication is not scrambled or encrypted and it is the radio portion of a cellular telephone, public land mobile radio service or paging service communication, then the violator will be subject to a $500 criminal fine. Otherwise, as stated in clause (i) of proposed paragraph 2511(4)(b), the conduct is punishable as a one-year misdemeanor with fines of up to $100,000, 18 U.S.C. 3623, unless the conduct is that described in subsection (5).

It should be noted that the exceptions set out in proposed paragraph 2511(4)(b) apply only to radio communications. The interception of "wire" communications remain punishable as five-year felonies. The interception of the wire portion of a cellular telephone call, for example, is a five-year felony.

Proposed paragraph 2511(4)(c) decriminalizes certain conduct unless it is for the purposes of direct or indirect commercial advantage or private financial gain. The terms "direct or indirect commercial advantage or private financial gain" are intended to have the same meaning as those terms have when they are used in 47 U.S.C. 705(b).

This exception from the criminal provisions of the Electronic Communications Privacy Act applies to the interception of an unencrypted, unscrambled satellite transmission that is transmitted (i) to a broadcasting station for purposes of retransmission to the general public; or (ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls. The conduct described in subparagraphs (i) and (ii) is not an offense under this chapter and is not subject to civil liability under this chapter.

Subparagraph (i) decriminalizes the interception of "network feeds" under title 18. Such conduct will be governed exclusively by section 705 of the Communications Act (47 U.S.C. 705).

Subparagraph (ii) decriminalizes the interception of material transmitted as an audio subcarrier provided that the information is intended for redistribution to facilities open to the public. Audio subcarriers intended for redistribution to facilities open to the public include those for redistribution by broadcast stations, cable TV systems and like facilities. They also include those for redistribution to buildings open to the public, and thus, it would not be unlawful to intercept music transmitted via an audio subcarrier if it is intended for redistribution to buildings like hospitals and office buildings which pump music into their lobbies and other public areas.

Subparagraph (ii) does not apply to data transmissions or telephone calls. The interception of those transmissions, like the interception of transmissions made for the enumerated bad purposes, would be punishable as 5-year felonies.

The private viewing of satellite cable programming, network feeds and certain audio subcarriers will continue to be governed exclusively by section 705 of the Communications Act of 1934, as amended, and not by chapter 119 of title 18 of the United States Code.

A new government action for injunctive relief is set out in proposed subsection 2511(5) of title 18. This new subsection was created to underscore that this public injunctive action is distinct from the criminal penalties set out in subsection (4).

Its exceptions apply only if the communication is not scrambled or encrypted and the conduct is not for one of the enumerated bad purposes. Clause (A) refers to the private or home viewing of a private satellite video communication. With regard to the home viewing of private satellite video communications, for purposes of this provision and proposed section 2520, the Committee views as scrambling that type of multiplexing [8] in which the audio and video portions of a communication are split, requiring special equipment to reassemble the whole communication (generally a videoteleconference) before it can be received in intelligible form. Clause (B) refers to radio communications transmitted on frequencies allocated under subpart D of part 74 of the FCC rules.

Under proposed clause 2511(5)(a)(ii)(A), if the violation is a first offense and the person has not previously been found liable in a private civil action under section 2520 of title 18, the government may sue for appropriate injunctive relief. Under proposed clause (B) if the violation is a second or subsequent offense or the person has previously been found liable under section 2520, he shall be subject to a mandatory $500 civil fine.

Proposed paragraph (b) of subsection 2511(5) clarifies that the court may use any means within its existing authority, including civil or criminal contempt, to enforce an injunction issued to an individual under this subsection. Paragraph (b) also requires that the court impose a civil fine of $500 or more for each violation of such

[8] Multiplexing refers to the transmission of communications by means of [illegible] techniques where [illegible] parameters have been withheld from the public.

an injunction. The term "violation" in this context refers to each viewing of a private video communication and to each reception of a part 74 D radio communication.

Subsection 101(e)—Exclusivity of remedies with respect to electronic communications

Subsection 101(e) of the Electronic Communications Privacy Act amends subsection 2518(10) of title 18 to add a paragraph (c) which provides that with respect to the interception of electronic communications, the remedies and sanctions described in this chapter are the only judicial remedies and sanctions available for nonconstitutional violations of this chapter involving such communications. In the event that there is a violation of law of a constitutional magnitude, the court involved in a subsequent trial will apply the existing Constitutional law with respect to the exclusionary rule.

The purpose of this provision is to underscore that, as a result of discussions with the Justice Department, the Electronic Communications Privacy Act does not apply the statutory exclusionary rule contained in title III of the Omnibus Crime Control and Safe Streets Act of 1968 to the interception of electronic communications.

Similarly, the Electronic Communications Privacy Act does not amend the Communications Act of 1934. Conduct in violation of that statute, will continue to be governed by that statute.

Subsection 101(f)—State of mind

Subsection 101(f) of the Electronic Communications Privacy Act changes the state of mind required to violate section 2511 or section 2512 of title 18 of the United States Code from "willful" to "intentional." The purpose of this amendment is to underscore that inadvertent interceptions are not crimes under the Electronic Communications Privacy Act.

As used in the Electronic Communications Privacy Act, the term "intentional" is narrower than the dictionary definition of "intentional." "Intentional" means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective. An "intentional" state of mind means that one's state of mind is intentional as to one's conduct or the result of one's conduct if such conduct or result is one's conscious objective. The intentional state of mind is applicable only to conduct and results. Since one has no control over the existence of circumstances, one cannot "intend" them.

As indicated in the Judiciary Committee's report to accompany the Criminal Code Reform Act of 1981 (S. 1630):

> The highest degree of culpability is present if a person engages in conduct (or causes a result) *intentionally*, that is, "if it is his conscious objective or desire to engage in the conduct (or cause the result)." A common means to describe conduct as intentional, or to say that one causes the result intentionally, is to state that it is done or accomplished "on purpose."

> The term "intentional" is not meant to connote the existence of a motive. Liability for intentionally engaging in prohibited conduct is not dependent on an assessment of the merit of the motive that led the person to disregard the law. (Emphasis in original; citation omitted.) Report of the Committee on the Judiciary, United States Senate, to accompany S. 1630, Criminal Code Reform Act of 1981, Report 97-307 at 67.

The Committee went on to point out that people who steal because they like to or to get more money or to feed the poor, like Robin Hood, all commit the same crime. Id. The word "intentional" describes the mental attitude associated with an act that is being done on purpose. It does not suggest that the act was committed for a particular evil purpose.

At this point, it is important to note that the crime of interception under the Electronic Communications Privacy Act consists of the intentional acquisition of the contents of a wire, electronic or oral, communication through the use of any electronic, mechanical, or other device. Some groups which engage in testing were concerned that the picking up of the contents of a communication incident to those tests might be considered a crime under title III as amended by the Electronic Communications Privacy Act.

They then sought exemptions from liability under proposed paragraph 2511(2)(g). The Subcommittee on Patents, Copyrights and Trademarks rejected this approach solely because it feared application of the principle of statutory construction of "expressio unius, est exclusio alterius" would encourage courts to treat similar tests as unlawful.

For example, since the early 1960s, motor vehicle manufacturers and others have been committed to voluntary actions to make their products "good citizens" in the electromagnetic environment. That commitment has fostered the development of test procedures and programs resulting in systems to help ensure that the electromagnetic energy radiated from equipment such as motor vehicles, agricultural and construction machinery, engines for transportation, marine, industrial and consumer applications, electronic equipment and components of the foregoing do not interfere with signals carrying video, voice or data transmissions. Personal, business and entertainment radio, television, digital data communications, and radio navigation services are examples of services benefited by such test procedures and programs.

The equipment for measuring the test procedures and technical specifications by which electromagnetic radiation from motor vehicles typically includes an antenna for picking up electromagnetic energy radiated from the vehicle, and a radio receiver for scanning the frequency range from 20 or 30 to 1,000 MHz to determine the field strength of all emissions in that range which the antenna picks up.

The antenna picks up not only the electromagnetic emissions from the equipment being tested, but also any other signals present at the antenna location. Indeed, to be able to quantify the strength of the emissions to be measured, even though additional signals are present at the frequency on which the measurement is being made,

the procedures and programs specify initial measurement of these additional signals. Of course, any radio service operating in the scanned frequency range will be picked up and its field strength measured during both the baseline and the vehicle tests. Although occasionally a speaker will be used to verify that a radio service is indeed producing a high field strength reading, in virtually all of the testing there is not attempt to ascertain the substance, purport or meaning of the signal.

Similar equipment and procedures are used to measure electromagnetic radiation emitted by computing devices. In addition, the operation of electronic equipment, and devices equipped with electronic controls, may be susceptible to disruption by electromagnetic radiation impinging on such equipment or devices. For example, the operation of electronic engine controls, electronic speed controls, and anti-lock brake systems employing electronic controls, and even the operation of heart pacemakers, are potentially susceptible to disruption by strong electromagnetic radiation.

To help design equipment and devices which are resistant to such disruption, such equipment and devices customarily are irradiated during their development with electromagnetic engery at a variety of radio frequencies, and the effects, if any, of such irradiation on their operation are observed. To avoid interference with ongoing radio services, it is essential that the test engineer, before turning on the radio transmitter used for such irradiation, listen on the transmitter frequency to ascertain that there is no other signal on that frequency with which the test transmission might interfere.

In addition, both the EPA and the FCC have pointed out that Federal agencies and state and local governments are currently addressing the problem of potentially excessive public exposure to radio frequency (RF) radiation emitted by various kinds of equipment. Testing solely to determine the source of, or to measure, RF emissions in order to comply with or to establish or enforce applicable federal, state or local standards limiting human exposure to RF radiation is not prohibited by the Electronic Communications Privacy Act.

This legislation was never intended to outlaw such testing, conducted in the ordinary course of the tester's business or regulatory activities. However, if one who obtained information in the course of such a test went beyond the procedures of the test to use any information obtained through the testing process, he could violate this statute.

Section 102—Requirements for certain disclosures

Section 102 of this legislation amends section 2511 of title 18 of the United States Code to add a new criminal prohibition on disclosure of electronic communications. It adds a new subsection (3) to section 2511. This amendment includes the term "to the public." The Government is included as part of the public. Thus, FTS services are covered.

The language in paragraph (a) of proposed subsection 2511(3) of title 18 provides that a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or the agent of such addressee or intended recipient.

Proposed paragraph (b) of new subsection 2511(3) of title 18 sets out exceptions to paragraph (a)'s criminal prohibition on disclosure. Providers of electronic communication services to the public are permitted to divulge the contents of any such communication (i) as otherwise authorized in section 2511(2)(a) or 2517 or title 18; (ii) with the lawful consent of the originator or any addressee or intended recipient; (iii) to any person employed or authorized, or whose facilities are used, to forward such communication to its destination, or (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime if such divulgence is made to a law enforcement agency.

The exceptions to the divulgence bar are relatively straightforward. Providers should be permitted to divulge under other provisions of the chapter. To be consistent with the one party consent exception found in the chapter, a similar exception is appropriate here. It is also logical to provide an exception with respect to activities necessary and intrinsic to the communication activity. Therefore, it is necessary to exempt communication intermediaries.

Finally, if an electronic communications service provider inadvertently obtains the contents of a communication during transmission and the communication appears to relate to the commission of a crime, divulgence is permitted when such divulgence is made to a law enforcement agency. If the provider purposefully sets out to monitor conversations to ascertain whether criminal activity has occurred, this exception would not apply.

Section 103—Recovery of civil damages

Section 103 of the Electronic Communications Privacy Act amends existing section 2520 of title 18 of the United States Code to incorporate violations involving interception, disclosure or intentional use of wire, oral, or electronic communications.

Proposed subsection 2520(a) of title 18 authorizes the commencement of a civil suit. There is one exception. A civil action will not lie where the requirements of section 2511(2)(a)(ii) of title 18 are met. With regard to that exception, the Committee intends that the following procedural standards will apply:

(1) The complaint must allege that a wire or electronic communications service provider (or one of its employees): (a) disclosed the existence of a wiretap; (b) acted without a facially valid court order or certification; (c) acted beyond the scope of a court order or certification or (d) acted on bad faith. Acting in bad faith would include failing to read the order or collusion. If the complaint fails to make any of these allegations, the defendant can move to dismiss the complaint for failure to state a claim upon which relief can be granted.

(2) If during the course of pretrial discovery the plaintiff's claim proves baseless, the defendant can move for summary judgment.

(3) If the court denies the summary judgment motion, the case goes to trial. At the close of the plaintiff's case, the de-

fendant again can move for dismissal. If that motion is denied, the defendant then has the opportunity to present to the jury its section 2520 good faith defense.

The plaintiff may bring a civil action under section 2520 whether or not the defendant has been subject to a criminal prosecution for the acts complained of, but in the absence of such prosecution and conviction, it is the plaintiff's burden to establish that the requirements of this section are met.

Proposed subsection 2520(b) indicates that appropriate relief in a civil action can include: (1) preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection (c) and punitive damages in appropriate cases, and (3) a reasonable attorney's fee and other reasonable litigation costs.

Proposed subsection 2520(c) provides a method for the computation of damages. The general rule is set out in paragraph (2) of subsection (c). The court may assess damages consisting of whichever is the greater of (A) the sum of the plaintiff's actual damages and any profits the violator made as a result of the violation; or (B) statutory damages of whichever is the greater of $100 a day or $10,000.

An exception from that general rule is set out in proposed paragraph (1) of subsection 2520(c). This exception applies if the violation consists of the private or home viewing of an unencrypted or unscrambled private satellite video communication or if the communication is an unencrypted or unscrambled radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the FCC rules, and the conduct is not for one of the enumerated bad purposes.

Under subparagraph (A), if the violator has not previously been enjoined in a government action under subsection 2511(5) and has not been found liable in a prior civil action, the court shall assess the greater of the sum of the plaintiff's actual damages or statutory damages of $50 to $500. Under subparagraph (B), if the violator is a second offender (one who has been found liable in a prior private civil action under section 2520 or one who has been enjoined in a government suit), the court shall assess the greater of the sum of the plaintiff's actual damages or statutory damages of $100 to $1000. Third and subsequent offenders are subject to the bill's full civil penalties as described in the general rule set out in proposed paragraph 2520(c)(2).

Subsection 2520(d) provides a good faith defense for those who comply with court orders or warrants, grand jury subpoenas, legislative or statutory authorizations, or a request of an investigative or law enforcement officer under section 2518(7) of title 17 concerning emergency situations. As used in this subsection, the term "good faith" includes the receipt of a facially valid court order. The fact that the provider of a wire or electronic communication service received a facially valid court order means that the provider would be entitled to a dismissal of a civil action upon a showing that he acted within the scope of that order.

Proposed subsection 2520(e) sets out the statute of limitations for actions brought under this section. Actions may not be commenced more than 2 years after the date on which the claimant first has a reasonable opportunity to discover the violation.

Section 104—Certain approvals by justice department officials

Section 104 of the Electronic Communications Privacy Act amends section 2516(1) of title 18 of the United States Code to add to the list of Federal officials who may make applications for court orders under chapter 119. Under this amendment, the list of officials who may be specially designated by the Attorney General to authorize applications will include any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division. The addition of an acting Assistant Attorney General is not meant to imply rejection in any other context of the well-established principle that an acting official ordinarily possesses all the legal powers of the official for whom he is acting, but to clarify the law under this statute.

As indicated in proposed subsection 111(c) of the Electronic Comunications Privacy Act, this section 104 shall take effect on the date of enactment.

Section 105—Addition of offenses to crimes for which interception is authorized

Section 105 of the Electronic Communications Privacy Act amends existing section 2516 of title 18 to add to the list of felonies for which a wiretap or bugging order may be obtained under chapter 119. It also adds a new subsection (3) to section 2516 which addresses applications and orders for interceptions of electronic communications.

Subsection 105(a)—Offenses for which wire and oral interceptions are authorized

Subsection 105(a) of the legislation amends subsection 2516(1) of title 18 by adding to the list of predicate felonies for which an application for a wiretapping or bugging order may be made. Those crimes are set out in the bill.

Subsection 105(b)—Offenses for which interception of electronic communication are authorized

Subsection 105(b) of the Electronic Communications Privacy Act amends section 2516 to authorize the Government to apply for a court order authorizing or approving the interception of an electronic communication by an investigative or law enforcement officer when an interception may provide or has provided evidence of a Federal felony. Thus, for non-wire, non-oral electronic communications, a different and less restrictive list of crimes can be used to justify an application for interception.

The Department of Justice has advised the Committee on the Judiciary that for the three years which follow the date of enactment of this legislation, this authority will only be exercised pursuant to the approval of the same level of officials as those involved in the approval of applications for wire interceptions. In addition to this voluntary regulatory limitation, the Department of Justice has committed itself to submitting to the relevant congressional committees any proposed changes in these regulations at least 90 days in advance of any change.

Section 106—Applications, orders, and implementation of orders

Section 106 of the Electronic Communications Privacy Act amends section 2518 of title 18 of the United States Code. This section addresses the implementation of interception orders, reimbursement for providers who assist law enforcement agencies in carrying out an interception order and minimization requirements. Subsection 106(d) of the legislation permits law enforcement agencies to request an order for a "roving tap" under certain limited circumstances.

Telephone companies have, as a matter of practice, provided information and technical assistance to law enforcement officials in connection with lawfully authorized wiretaps. They have steadfastly maintained, however, an important distinction between such technical assistance and any active participation in the wiretap itself.

Section 2518(4) of title 18 is a codification of the cooperative working relationship that exists between telephone companies and law enforcement officials. This section anticipates that these government officials will, and should, seek the cooperation of telephone companies in accomplishing telephone line interceptions.

Nevertheless, telephone company customers have a reasonable expectation, traditionally enhanced by telephone company practices and policies, that their company will not become in effect, a branch of Government law enforcement. Accordingly, while technical assistance is provided and paid for, the Committee wishes to make clear that Section 2518(4) is not intended to authorize and should not be construed as authorizing, issuance of an order for land line telephone company assistance which either requires a company to actually accomplish or perform a wiretap or requires that law enforcement wiretap activity take place on land line telephone company premises.

The Committee understands that some cellular service providers may have cooperated with law enforcement officials to establish wiretap connections on the cellular service provider's premises. The Committee does not intend to alter this specific form of assistance.

The Committee understands that the practice followed with regard to land line telephones is that telephone company employees do not perform the wiretap itself, and that telephone company premises are not used for wiretap activity. This procedure is accepted by both company and law enforcement officials. The Committee does not expect any departure from current practice.

To ensure that the practice does not change, absent a compelling need appropriately addressed to Congress, the Committee expects the Justice Department to include in its United States Attorneys Manual a statement that no enforcement agency or official shall attempt to compel any telephone company employee to perform any wiretap, or attempt to compel any such company to make its premises available for wiretap activity. Any proposed amendment to that language should be reported to the Committee well in advance of dissemination so that the Committee has sufficient opportunity to assess both the extent of which such proposed language comports with its view of the scope of section 2518(4) as expressed above and the extent to which any amendment of section 2518(4) to permit a change in prevailing practice may be warranted by subsequent and compelling changes in technology or other circumstances.

Subsection 106(a)—Place of authorized interception

Subsection 106(a) of the Electronic Communications Privacy Act amends subsection 2518(3) of title 18. It provides, that in the case of a mobile interception device, a court can authorize an order within its jurisdiction and outside its jurisdiction but within the United States. This provision applies to both a listening device installed in a vehicle and to a tap placed on a cellular or other telephone instrument installed in a vehicle.

In most cases, courts will authorize the installation of a device and the device will be installed within the court's jurisdiction, but the suspect will subsequently move outside that jurisdiction. In certain cases, however, a device authorized for installation in an automobile may be authorized in one district and the vehicle might be moved to another district prior to installation. Subsection 106(a) of the bill permits installation in the district to which the vehicle has been moved.

Nothing in this subsection affects the current law with regard to the use of such devices outside the United States.

Subsection 106(b)—Reimbursement

Subsection 106(b) of the Electronic Communications Privacy Act establishes that service providers that provide assistance to the agency carrying out an interception order may be compensated for reasonable expenses incurred in providing such facilities or assistance. This is designed to permit reimbursement at an amount appropriate to the work required. In most cases, a flat or general rate will be appropriate, but this change in the existing law will permit flexibility by authorizing reimbursement at a higher level in unusual cases.

Subsection 106(c)—Minimization

This subsection makes two changes in section 2518(5) of title 18. Under existing law, no section 2518 interception order may extend longer than 30 days. Paragraph (1) of subsection 106(c) provides a rule for establishing when the 30 days to install a tap or a bug begins to run. Under this rule, the 30-day time period commences on the earlier of the day on which the officer first begins to conduct the interception, or 10 days after the order is entered.

Paragraph (2) of this subsection of the Electronic Communications Privacy Act provides a special minimization rule for intercepted communications that are in code or in a foreign language. If an expert in that foreign language or code is not reasonably available during that interception period, minimization may be accomplished as soon as practicable after the interception. In this regard, it is contemplated that the translator or decoder will listen to the tapes of an interception and make available to the investigators the minimized portions preserving the rest for possible court perusal later.

Paragraph (2) also provides that the monitoring of interceptions under this chapter may be conducted in whole or in part by Government personnel, or by individuals operating under contract with the Government, as long as such personnel are acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception. This change, which was sought by the Federal Bureau of Investigation, is designed to free field agents from the relatively routine activity of monitoring interceptions so that they can engage in other law enforcement activities.

The Committee recognizes that although the statutory standards for minimizing wire, oral, and electronic communications are the same under proposed subsection 2518(5), the technology used to either transmit or intercept an electronic message such as electronic mail or a computer data transmission ordinarily will not make it possible to shut down the interception and taping or recording equipment simultaneously in order to minimize in the same manner as with a wire interception. It is impossible to "listen" to a computer and determine when to stop listening and minimize as it is possible to do in listening to a telephone conversation. For instance, a page displayed on a screen during a computer transmission might have five paragraphs of which the second and third are relevant to the investigation and the others are not. The printing technology is such that the whole page including the irrelevant paragraphs, would have to be printed and read, before anything can be done about minimization.

Thus, minimization for computer transmissions would require a somewhat different procedure than that used to minimize a telephone call. Common sense would dictate, and it is the Committee's intention, that the minimization should be conducted by the initial law enforcement officials who review the transcript. Those officials would delete all non-relevant materials and disseminate to other officials only that information which is relevant to the investigation.

Subsection 106(d)—Roving taps

This subsection of the Electronic Communications Privacy Act adds a new subsection (11) to section 2518 of title 18. Under current law, the application and the order for a bug or tap must indicate the "particular" facility or place in which the interception is to occur. Subsection 106(d) of this legislation sets out new rules for the specificity required in the description of the place where the interceptions of wire and oral communications are to occur. The Committee finds such a provision necessary to cover circumstances under which law enforcement officials may not know, until shortly before the communication, which telephone line will be used by the person under surveillance. Telephone companies assist law enforcement officials by providing cable and pair information, or leased line facilities when requested and feasible. this is the information which will be provided to law enforcement for roving taps.

In the case of both oral and wire communications, only a limited list of Federal officials can apply for a special order seeking relief under this provision.

With regard to "oral" communications, as set out in paragraph (a) of proposed subsection 2518(11), an application for a special

order must contain a full and complete statement as to why the ordinary specification requirements are not practical. The application must also identify the person committing the offense and whose communications are to be intercepted. The judge must find that the ordinary specification rules are not practical. Situations where ordinary specification rules would not be practical would include those where a suspect moves from room to room in a hotel to avoid a bug or where a suspect sets up a meeting with another suspect on a beach or a field. In such situations, the order would indicate authority to follow the suspect and engage in the interception once the targeted conversation occurs.

The rule with respect to "wire communications" is somewhat similar. As indicated in paragraph (b), the application must show that the person committing the offense has a purpose to thwart interception by changing facilities. In these cases, the court must find that the applicant has shown that such a purpose has been evidenced by the suspect. An example of a situation which would meet this test would be an alleged terrorist who went from phone booth to phone booth numerous times to avoid interception. A person whose telephone calls were intercepted who said that he or she was planning on moving from phone to phone or to pay phones to avoid detection also would have demonstrated that purpose.

Proposed subsection 2518(12) of title 18 provides, with respect to both "wire" and "oral" communications, that where the federal government has been successful in obtaining a relaxed specificity order, it cannot begin the interception until the facilities or place from which the communication is to be intercepted is ascertained by the person implementing the interception order. In other words, the actual interception could not begin until the suspect begins or evidences an intention to begin a conversation.

It would be improper to use this expanded specificity order to tap a series of telephones, intercept all conversations over such phones and then minimize the conversations collected as a result. This provision puts the burden on the investigation agency to ascertain when the interception is to take place.

The Subcommittee on Patents, Copyrights and Trademarks added a provision to proposed subsection 2518(12) allowing a service provider to move the court to modify or quash the order on the grounds that it cannot provide assistance in a timely or reasonable manner. As indicated, on notice to the Government, the court must decide such a motion expeditiously.

This provision recognizes that a telephone company may not be able to respond instantaneously to an eleventh hour target line designation. It is designed to account for the practicalities of telephone company response time, the number of phones that may be covered by the order, and the geographic area of the target lines that may be used by the person under surveillance.

The Committee intends that the court look to several factors in considering whether to issue an order pursuant to proposed paragraph (11)(b). The request for the order, and the order itself, should specify a reasonably limited geographic area, the number of phones (and phone numbers) if known, to be intercepted—so as not to render telephone company cooperation technically infeasible—and the time within which the interception is to be accomplished. The

failure to make such specifications in the request and/or in the order may be considered evidence of unreasonableness or untimeliness by a court acting upon a telephone company motion made pursuant to proposed subsection (12).

The Committee also expects law enforcement officials to continue the current practice of consulting with telephone company employees regarding the details of implementation (such as phone numbers and the specific locations of the telephones) in advance of the time any order for interception is sought.

Finally, subsection 106(d) of the Electronic Communications Privacy Act provides that reports to the Administrative Office of the United States Courts under current section 2519 of title 18 on the kind of order or extension applied for include whether or not the order was one applied for under the relaxed specifity provisions of subsection 2518(11).

Section 107—Intelligence activities

Subsection (a) of this section of the bill clarifies that the amendments made in subsection 102(b) of the bill do not provide any new authority for intelligence activities but only represent an exemption from the coverage of this chapter and chapter 121 of title 18 for activities that are otherwise lawful.

Subsection (b) of this section of the bill exempts communications security monitoring activities of the Federal Government otherwise in accordance with U.S. law and undertaken in accordance with procedures approved by the Attorney General from coverage under chapter 119 or 121 of title 18. This subsection provides no new authority for such activities.

Specifically this subsection exempts from the coverage of this act the lawful activities of Federal agencies intended to intercept encrypted or other official communications for communications security purposes. Communications security measures are protective measures taken to deny unauthorized persons information derived from U.S. Government telecommunications and to ensure the authenticity of such communications. Communications security protection is the application of security measures to electrical systems generating, handling, processing, or using information the loss of which could adversely affect the national interest. Monitoring of security measures and security protection includes the intentional interception of executive branch official communications, including the communications of certain Government contractors, to provide technical material for analysis to determine the degree of security being provided to these transmissions. In addition, the interception, by authorized Federal agencies, of radio communications between foreign powers or agents as defined by the Foreign Intelligence Surveillance Act of 1978, and the accessing of electronic communications systems used exclusively by a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978, are exempted from coverage of this act by this subsection of the bill.

Section 108—Mobile tracking devices

Subsection (a) of this section of the bill adds a new section to chapter 205 of title 18. This new code section provides that if a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, and the tracking of the object or person on which the device is installed, such warrant remains valid even if the device is moved outside the jurisdiction of the court, even outside the jurisdiction of the United States, provided that the device was installed within the jurisdiction of the court, in conformity with the court order. This clarification does not effect current legal standards for the issuance of such an order.

A tracking device is defined as an electronic or mechanical device which permits the tracking of the movement of a person or object.

Subsection (b) adds a new section 3117, "Mobile tracking devices" to the table of contents of chapter 205.

Section 109—Warning subject of surveillance

The section amends section 2232 of title 18 by adding at the end a new subsection. Proposed subsection 2232(c) adds two new offenses to title 18. First, it makes it a criminal act punishable by a fine under this title and/or imprisonment for not more than 5 years to warn any person that a Federal agency or law enforcement officer has been authorized or has sought authorization under chapter 119 of title 18 to intercept a wire, oral, or electronic communication. Second, the proposed subsection provides the same penalties for warning anyone that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the provisions of the Foreign Intelligence Surveillance Act.

The elements of both new crimes are the same. It is required that the defendent have knowledge that the Federal law enforcement or investigative officer has been authorized or has applied for an interception order. The defendent need not know that such an application was made under a particular chapter of federal law, rather, only that such application or order was made under federal law. The defendent must engage in conduct of giving notice of the possible interception to any person who was or is the target of the interception. Finally, the defendents action must have been undertaken with the specific intent to obstruct, impede or prevent the interception. The offense also includes an attempt to engage in the offense.

Section 110—Injunctive remedy

This section of the act sets out a proposed section 2521 of title 18. Section 2521 adds to the existing criminal and civil remedies available for violations of this chapter by authorizing the Attorney General to seek an injunction to prevent felony level violations of this chapter. Section 2521 also provides that preliminary relief can be granted to prevent a continuing and substantial injury to the United States or to any person for whose protection the action is brought. Actions under section 2521 are governed by the Federal Rules of Civil Procedure, except that when an indication has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

Section 111—Effective date

Subsection (a) provides that in general the amendments made by this act are effective 90 days after enactment, and that the act applies only with respect to court orders or extensions made after the effective date. Thus existing court orders would not be affected by these changes and on-going investigations would not be hindered, but any extention of an existing court order made 90 days after passage would be governed by these new provision.

Subsection (b) provides a special rule for the effective date in the case of state authorizations of interceptions. This special effective date rule is necessary because the provisions of chapter 119 of title 18 supersede state laws with respect to electronic communications. Under chapter 119, the states must enact statutes which are at least as restrictive as the provisions of chapter 119 before they can authorize their state courts to issue interception orders. Because of the substantial changes made by this act it is appropriate to grant the states sufficient time to modify their laws. This special effective date rule gives the states two years to amend their laws to meet the new requirements of chapter 119.

Subsection (c) provides that section 104 of the act is effective upon enactment. Section 104 modifies Justice Department procedures for approval of requests under this chapter, since section 104 is designed to alleviate management difficulties at the Department of Justice there is no reason to delay implementation of these changes.

TITLE II—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Section 201—Title 18 amendment

This section amends title 18 by adding at the end thereof a new chapter 121 consisting of ten new sections. These sections are discussed below.

New section 2701—Unlawful access to stored communications

Subsection (a) of this new section creates a criminal offense for either intentionally accessing, without authorization, a facility through which an electronic communication service is provided, or for intentionally exceeding the authorization for accessing that facility. Subsection 2701, also provides that the offender must obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such an electronic storage system in order to commit a violation under the subsection. The term "electronic storage" is defined in section 2510(17) of title 18 and includes both temporary, intermediate storage of a wire or electronic communication incidental to the transmission of the message, and any storage of such a communication by the electronic communication service for purposes of backup protection of the communication.

This provision addresses the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public.

This subsection does not prevent broad authorizations to the general public to access such a facility. The bill does not for example hinder the development or use of "electronic bulletin boards" or other similar services where the availability of information about the service, and the readily accessible nature of the service are widely known and the service does not require any special access code or warning to indicate that the information is private. To access a communication in such a public system is not a violation of the Act, since the general public has been "authorized" to do so by the facility provider.

However, the offense of intentionally exceeding an authorization to access a computer facility would apply both to public and private aspects of a system. For example, a computer mail facility authorizes a subscriber to access information in their portion of the facilities storage. Accessing the storage of other subscribers without specific authorization to do so would be a violation of this provision. Similarly, a member of the general public authorized to access the public portion of a computer facility would violate this section by intentionally exceeding that authorization and accessing the private portions of the facility.

Subsection (b) of this new section provides punishment for violation of subsection (a). A distinction is drawn between offenses committed for purposes of commercial advantage, malicious destruction or damage, or for private commercial gain and all other types of violation. If the offense is committed for private or commercial gain or for malicious destruction the subsection provides a fine of not more than $250,000 or imprisonment for not more than one year, or both, for a first offender. Second and subsequent offenders are subject to the same fine provision but a jail term up to two years can be imposed for such violations. In all other cases the fine is limited to not more than $5,000 and imprisonment for not more than 6 months or both.

Subsection (c) of this new section provides exceptions to the violations contained in subsection (a). It is not a violation of subsection (a) if the conduct was authorized by the person or entity providing the wire or communications service, or if the conduct was authorized by the user of that service with respect to communications of or intended for that user or if the conduct is authorized by new sections 2703, 2704, or 2518 or title 18.

New section 2702—Disclosure of contents

Proposed section 2702 is divided between electronic communication services and remote computing services. The restrictions on the service provider are the same in each instance. However, as described below, there is different treatment for electronic communication service providers and remote computing services with regard to government access.

Subsection (a) of this new section prohibits the provider of an electronic communications service or the provider of a remote computing service from knowingly divulging the contents of any communication. The "contents" of a communication has the same meaning in this section as it has in subsection 2510(8) of title 18 or the United States Code as amended by section 101(a)(5) of this Act. The requirement that a violator must "knowingly" divulge the con-

tents is intended to make clear that "reckless" or "negligent" conduct is not sufficient to constitute a violation of this section. Subsection (b) of this section provides exceptions to this general rule of non-disclosure.

The application of new code section 2702(a) generally prohibits the provider of a wire or electronic communication service to the public from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient. Similarly, section 2511(3) of title 18, as amended by this Act, prohibits such a provider from divulging the contents of a communication while it is in transmission. Neither provision, however, nor any other provision in the Act, is intended to affect any other provision of federal law that prohibits the disclosure of information on the basis of the content of the information, such as the Fair Credit Reporting Act.

The application of sections 2701(a) and 2511(3) is limited to providers of wire or electronic communications services. There are instances, however, in which a person or entity both acts as a provider of such services and also offers other services to the public. In some such situations, the bill may allow disclosure while another federal requirement, applicable to the person or entity in another of its roles, prohibits disclosure. The Committee intends that such instances be analyzed as though the communication services and the other services were provided by distinct entities. Where a combined entity in its non-provider role would not be allowed to disclose, the appropriate outcome would be non-disclosure.

Subsection (b) of this new section provides exceptions to the general rule of nondisclosure provided in subsection (a). These exceptions permit disclosure: (1) to the addressee or intended recipient of the communication or the authorized agent of such addressee or intended recipient; (2) in conformity with a court order issued pursuant to the procedures in section 2516 of title 18; or in the course of normal business practice as defined in section 2511(2)(a) of this title; or to the government under procedures of new section 2703; (3) with the lawful consent of the sender or the addressee or an intended recipient of such communication or with the consent of the subscriber in the case of a remote computing service; (4) to a person employed or authorized or whose facilities are used to forward the communication to its ultimate destination; (5) as necessary in order to render the service or to protect the rights or property of the provider of the service: of (6) to a law enforcement agency, if the contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime

The exceptions to the general rule of nondisclosure provided in subsection (b) fall into three categories. The first category are those disclosures which are authorized by either the sender or receiver of the message. Either the sender or the receiver can directly or through authorized agents authorize further disclosures of the contents of their electronic communication. The second category are disclosures which are necessary for the efficient operation of the communications system. Such business procedures are included in the section 2511(2)(a) exemption as well the exemptions of this subsection relating to the diclosure of the message to forwarding facilities and the exemption for service provider activities designed to protect the system and perform the service. The third category are disclosures to the government. In this area there are two types of disclosures. Those pursuant to a court order under the procedures of sections 2516 and 2703 and those disclosures undertaken at the initiative of the service provider in the exceptional circumstances when the provider has become aware of the contents of a message that relate to ongoing criminal activity.

New section 2703.—Requirements for governmental access

Subsection (a) of section 2703 provides requirements for the government to obtain the contents of an electronic communication that has been in electronic storage for 180 days or less. A government entity can only gain access to the contents of such an electronic communication pursuant to a warrant issued under the Federal Rules of Criminal Procedure or an equivalent State warrant.

Subsection (b) of section 2703 provides that for electronic communications that are maintained by a remote computing service and that have been in storage in an electronic communication service for more than 180 days the Government can gain access in several ways. If the Government wishes to obtain the contents of a communication without the required notice to the subscriber then the governmental entity must obtain a warrant issued under the Federal Rules of Criminal Procedure or an equivalent State warrant. With prior notice from the government entity to the subscriber or customer, the entity may obtain the contents of the electronic communication either by using an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena or obtain a court order pursuant to subsection (d) of this section. In addition, the required notice may be delayed pursuant to the requirements of section 2705 of title 18 as provided in the Act.

Subsection (b) of new section 2703 of title 18 is made applicable to all electronic communications held or maintained by the service provider on behalf of a customer or subscriber and received by means of electronic transmission as well as electronic communications in storage or computer processing if the provider is not authorized to access the contents of any communications for purposes other than storage or computer processing.

Subsection (c) provides for access to records or other information pertaining to a subscriber to or customer of an electronic communications or remote computer service, not including the content of electronic communications. This section permits the provider of the service to divulge, in the normal course of business, such information as customer lists and payments to anyone except a Government agency. It should be noted that the information involved is information about the customer's use of the service not the content of the customer's communications.

A provider of electronic communication service or remote computing service must disclose information pertaining to a subscriber or customer, but not the contents of any communications of that customer, to a Government entity only when the Government entity either (i) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury subpoena; (ii) obtains a warrant issued under the Federal Rules of Criminal Procedure or an equivalent state warrant; (iii) obtains a court

order for such disclosure under subsection (d) of this section; or (iv) has obtained the consent of the subscriber. A Government entity which receives customer records pursuant to one of these four alternatives is not required to provide notice to the subscriber or customer that it has requested or obtained this information.

Subsection (d) provides that orders requiring access by a Government entity to the contents of a wire or electronic communication or to the records or other information sought shall issue only if the governmental entity shows there is reason to believe the contents of the wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. This section provides no authority for the issuance of a state subpoena that is prohibited under the law of such state.

This subsection also permits the provider of the communications or remote computing service to move to quash or modify any other issued under this section if the information or records requested are unusually voluminous or compliance with the order would cause an undue burden on the provider. This specific standing for the service provider to contest an overly broad order is intended to protect the service provider from unduly burdensome requirements and to permit an impartial judicial officer to evaluate the appropriateness of the government's request.

Subsection (e)—No cause of action against a provider disclosing information under this chapter.

This subsection of the proposed new section provides a defense for the service provider, its employees and officers, from suits arising because of its disclosure of information pursuant to a warrant or other court order issued under this chapter.

New section 2704—Backup preservation

Subsection (a) of proposed section 2704 of title 18 provides that a Government entity may include in its subpoena or court order obtained pursuant to the provisions of new section 2703(b)(2) a requirement that the service provider create and maintain a duplicate copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the customer or subscriber, the service provider must create such a duplicate copy as soon as practicable and confirm to the Government entity that the duplicate file has been created. In all cases the service provider must create such a duplicate file within two business days after receipt by that provider of the subpoena or court order directing that such a duplicate file be created.

Paragraph (2) of this new subsection requires the Government entity to give notice to the subscriber or customer that such a duplicate file has been created and has been ordered to be provided to the Government. This notification to the customer or subscriber must be given within three days of the receipt of confirmation from the service provider (as required by subsection (a) above) that the duplicate file has been created, unless the Government agency has obtained permission to delay such notification pursuant to proposed subsection 2705(a).

Paragraph (3) also prohibits the service provider from destroying the backup copy until the information has been delivered to the Government entity or any proceedings, including all appeals, con-

cerning the Government's subpoena or court order have been resolved, whichever is later. The service provider is required to comply with the order and release the copy to the requesting Government entity no sooner than fourteen days after the Government entity has notified the subscriber or customer that it is seeking this information.

Paragraph (4) provides that the service provider should release the information to the Government only if the service provider has not received notice from its subscriber or customer that the subscriber or customer has challenged the Government's request and if the service provider has not itself challenged the request of the Government entity.

Finally, paragraph (5) provides that when a Government entity seeks to require the creation of the backup or duplicate copy under this subsection and the governmental entity further determines that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with the evidence this later determination is not subject to challenge either by the subscriber or customer or by the service provider.

While this subtitle provides the subscriber or customer, and in some circumstances the service provider a right to challenge the necessity for or scope of a court order, neither this section or any other section of this Act provides grounds to challenge the determination of the Government agency that no notification is to be given to the subscriber or customer of the mere creation of the duplicate file. The file is created and maintained by the service provider solely for the purpose of assuring that potential evidence is not tampered with or destroyed. Keeping the fact of the creation of this file secret does not harm any privacy interest since there are adequate safeguards included in the bill and in this chapter to control the actual release of the duplicate file to the Government agency.

Subsection (b) of proposed section 2704 provides a procedure for challenges to a court order by the subscriber or customer. The subscriber or customer whose records are sought can within 14 days after notification by the Government under subsection (a)(2) of this section file a motion to quash such subpoena or vacate such court order in an appropriate State or Federal court. The subscriber or customer challenging the subpoena or order must serve a copy of the motion on the governmental entity and provide written notice to the service provider that such a challenge has been initiated.

The subsection further provides that the application or motion must state that the applicant is the customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought and state the reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or state that there has not been substantial compliance with the provisions of this chapter in some other respect.

The service required by this subsection shall be made upon the governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, or office, or department specified in the notice which the customer has received pursuant to this chapter. The term "delivery" in this subsection has

the meaning given that term in the Federal Rules of Civil Procedure.

If a court determines that the customer or subscriber has complied with the requirements for such a motion including the requirements of "delivery" to the Government entity, then the court shall order the Government entity to file a sworn response to the motion or application. Such response may be in camera if the governmental entity includes in its response the reasons which make such an in camera review appropriate. If the motion and response provide insufficient information for the court to make a determination, the court may conduct such additional proceedings as it deems appropriate. Any additional proceedings and a decision on the challenge shall occur as rapidly as feasible, *i.e.* within 7 calendar days in all but the most unusual circumstances.

The subsection also provides that the court shall enforce the process if it finds that the applicant challenging the order or application is not the subscriber or customer for whom the records are maintained or if it finds that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry. If the court finds that the customer or subscriber challenging the order or application is the subscriber or customer for whom the records are maintained and that the records are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect, then the court shall order the process quashed

Finally, the subsection provides that a court order denying a motion or application under section 2704 shall not be deemed a final order and no interlocutory appeal may be taken by the customer or subscriber from such a denial.

In the event that there is no indictment then the person whose records are involved may move for the return of the records. Obviously, nothing precludes a customer or subscriber who is later the subject of a criminal proceeding from raising these issues again subject to the sanctions limitation of section 2708 of title 18.

New section 2705—Delayed notice

This proposed section provides procedures and requirements for implementation for a delay of notice to the customer or subscriber that his records are being sought or have been provided to a government entity.

Subsection (a) of this section 2705 provides that when a Government entity seeks or obtains access to the contents of an electronic communication by application for a court order notification can be delayed for an initial period of up to 90 days, if the Government entity requests such a delay and the court determines that there is reason to believe that the notification of the existence of the court order may have an adverse result as described in this subsection. Where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, a delay of notification for a period of not more than 90 days can be obtained upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result.

For purposes of a delay of notification, an adverse result is defined as (A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidating of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

In the case of an administrative or grand jury subpoena, the governmental entity is required to maintain a true copy of the required certification, and the certification can only be given by a "supervisory official". The subsection defines such an official as the investigative agent in charge of an agency's headquarters or regional office, or the assistant to such an agent or the equivalent, or the chief prosecuting attorney or the first assistant prosecuting attorney of an agency's headquarters or regional office, or the equivalent.

The subsection also provides that extensions of the delay period for not more than 90 days each may be granted by the court upon application or by certification by the government agency provided the requirements of subsection (b) of section 2705 are met for each extension.

When the delay period, including any extensions thereof, as provided in this subsection and subsection (b), has expired the governmental entity must serve upon, or deliver by registered or first-class mail to the customer or subscriber, a copy of the process or request together with notice that states the nature of the law enforcement inquiry and informs the customer or subscriber: (i) that the information maintained for such customer or subscriber by the service provider was supplied or requested by the Government agency and stating the date on which the information was supplied or requested; (ii) that notification to the customer of this action was delayed; (iii) what Government entity or court made the certification or determination that notification could be delayed; and (iv) which provision or provisions of this chapter allowed the delay.

Subsection (b) provides that if a governmental entity has delayed notice or has not been required to give notice under the provisions of section 2703, then the governmental entity may also apply to the court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, not to notify any person of the existence of the warrant, subpoena, or court order. The court is required to enter such an order to prevent disclosure by the service provider if notification of the existence of the warrant, subpoena, or court order will result in any of the five adverse results listed in this subsection. The entity must apply to a court for preclusion under this subsection, even if the underlying process—an administrative subpoena, for example—does not require a court order.

New section 2706—Cost reimbursement

This proposed section provides that when a governmental entity obtains the contents of communications, records or other information under the authority of sections 2702, 2703, or 2704, it shall pay to the person or entity assembling or providing the information a fee for reimbursement for the reasonably necessary direct costs. The section provides an exception to this general rule with regard to records or other information maintained by a communications

common carrier that relate to telephone toll records and telephone listings obtained under section 2703. No fee is normally required for access to such records. However, the court may order a payment if the court determines the information required is unusually voluminous. The amount of the fee provided in this subsection is to be mutually agreed upon by the governmental entity and the person or entity providing the information. If they are unable to reach an agreement, the court which issued the order for production of the information, or the court before which a criminal prosecution relating to the information would be brought if no court order was issued, is empowered to determine a reasonable fee.

New section 2707—Civil action

Subsection (a) of this proposed section provides that, except as provided in section 2703(e), any provider of electronic communication service, subscriber, or customer of such service aggrieved by any violation of this new chapter may recover from any person or entity—including governmental entities—who knowingly or intentionally violated this chapter.

Under subsection (b), appropriate relief in a civil action under this title includes: (1) such preliminary, declaratory, or other equitable relief as may be appropriate; (2) damages under the section including the sum of actual damages suffered by the plaintiff and any profits made by the violator as the result of the violation as provided in (c) with minimum statutory damages of $1,000; and (3) reasonable attorney's fees and other reasonable litigation costs.

The section also provides a defense to an action under this chapter. If the defendant's action was based on a good faith reliance on a court order or warrant, a grand jury subpoena, a legislative or statutory authorization; or a request of an investigative or law enforcement officer under section 2518(7) of this title, or if it was based on a good faith determination that section 1511(3) of this title permitted the conduct complained of, then this good faith reliance or determination is a complete defense to any civil or criminal action brought under this chapter or under any other law.

This new section also provides that any action under this section must be commenced not later than 2 years after the date upon which the claimant first discovered or had a reasonable opportunity to discover that a violation had occurred.

New section 2708—Exclusivity of remedies

The remedies and sanctions provided in this chapter are the only judicially available remedies and sanctions for nonconstitutional violations of the chapter.

New section 2709.—Counterintelligence access to telephone toll and transactional records

Section 2709 provides for FBI counterintelligence access to telephone toll and transactional records. This provision is substantially the same as language recently reported by the Intelligence Committee as section 503 of the Intelligence Authorization Act for Fiscal Year 1987. There are two differences. The first is that section 2709 applies not only to FBI requests for telephone subscriber information and toll billing information, but also to FBI requests

for electronic communication transactional records. This ensures that the FBI has the necessary authority with regard to subscriber information and toll billing information with respect to electronic communication services other than ordinary telephone service.

Section 2709 is a carefully balanced provision that remedies the defect in current law that the FBI cannot gain access on a mandatory basis to telephone toll records maintained by communications common carriers, for counterintelligence purposes. As a result, especially in states where public regulatory bodies have created obstacles to providing such access, the FBI has been prevented from obtaining these records, which are highly important to the successful investigation of counterintelligence cases.

The second difference concerns the standard that the FBI must meet before it can require a common carrier or service provider to supply the requested records. Section 2709 requires a certification by a designated FBI official that the information sought is relevant to an authorized foreign counterintelligence investigation and that there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978. Section 503 of the Intelligence Authorization Act for Fiscal Year 1987, as reported by the Intelligence Committee, contains a slightly different "reason to believe" standard requiring specific and articulable facts giving reason to believe that the target "is or may be" a foreign power or an agent of a foreign power.

Subsection 2709(a) of this proposed section provides that a wire or electronic communication service provider must comply with a request for subscriber information and toll billing records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section. It should be noted that this applies only to transactional records, not to the content of the electronic messages of a customer or subscriber.

Subsection 2709(b) provides that in order for the requirement to provide information in subsection (a) of this section to apply, the Director of the Federal Bureau of Investigation, or a specific person within the Bureau designated for this purpose by the Director, must certify in writing to the wire or electronic communication service provider that (1) the information sought is relevant to an authorized foreign counterintelligence investigation; and (2) that there are specific, articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act.

The House Judiciary Committee report on the Electronic Communications Privacy Act of 1986 does not discuss the meaning of the "reason to believe" standard in section 2709. It is essential, therefore, to clarify the intent of the Senate with respect to this item.

The "reason to believe" requirement in section 2709 is intended to be substantially less stringent than the requirement of "probable cause." It is intended that the application of the "reason to believe" requirement will be determined by a senior FBI official at the level of Deputy Assistant Director or above. It is intended that

in applying the "reason to believe" standard to a specific case, the FBI official may take into account any facts or circumstances that a prudent investigator would consider, so long as there is an objective, factual basis of the determination.

The Senate Select Committee on Intelligence has informed the Judiciary Committee that the language contained in the bill would not significantly affect the application of the current FBI investigative standard in this area. Further discussion of the investigatory standard in particular cases is contained in the reports of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence on FY 87 Intelligence Authorization Act (S. 2477 and H.R. 4759).

Subsection 2709(c) prohibits a service provider, or any officer, employee, or agent of the service provider from disclosing to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

Subsection 2709(d) permits the Federal Bureau of Investigation to disseminate such information only in conformance with guidelines approved by the Attorney General for foreign intelligence and foreign counterintelligence investigations. If the information is to be disseminated to another federal agency, it can only be disseminated if the information is clearly relevant to the authorized responsibilities of such agency.

Subsection 2709(e) further requires that on a semiannual basis the Director of the Federal Bureau of Investigation fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made by the Bureau under subsection 2709(b).

New section 2710—Definitions for chapter

Terms used in section 2510 retain the definitions given to each term by that section. The term "remote computing service" is defined to mean the provision to the public of computer storage, or computer processing services by means of an electronic communications system.

This section also provides for the change in the table of chapters of title 18 of the United States Code by adding chapter 121 to the table.

Section 202—Effective date

This section provides that the amendments made by Title II of the bill shall be effective 90 days after the date of enactment. It further provides that changes made by this title that apply to conduct pursuant to court order or extension, apply only with respect to court orders or extensions made after the effective date of the title.

TITLE III—PEN REGISTERS AND TRAP AND TRACE DEVICES

Title III of the Electronic Communications Privacy Act proposes to add a new chapter 206 to title 18 of the United States Code. This chapter will govern the use, application and issuance of orders for pen registers and trap and trace devices. Those terms are defined in proposed section 3126 of title 18. Briefly, a pen register is a device which can be attached to a telephone line for the purpose of decoding and recording the numbers dialed from that line. A trap and trace device is used to identify the originating number of an incoming wire or electronic communication. These devices do not identify or record the contents of the communciation.

Section 301—Pen registers and trap and trace devices

Subsection 301(a) of the Electronic Communications Privacy Act sets out the six proposed sections of title 18 governing pen registers and trap and trace devices.

New section 3121—General prohibition on use of pen registers and trap and trace devices

Subsection (a) of proposed section 3121 of title 18 contains a general prohibition against the installation or use of a pen register or trap and trace device without a court order. Such a court order may be obtained under section 3123 of title 18 or under the Foreign Intelligence Surveillance Act (FISA).

Proposed subsection 3121(b) contains exceptions to subsection (a)'s general prohibition against the use of pen registers and trap and trace devices. Providers of electronic or wire communication services may use pen registers or trap and trace devices if one of three conditions are met. The provider may use a pen register or trap and trace device (1) if it relates to the operation, maintenance, and testing of a wire or elecronic communication service, or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse or unlawful use of the service; (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward completion, or a user of that service from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user has been obtained.

Proposed subsection 3121(c) imposes a penalty for a knowing violation of subsection (a). The penalty is a fine under this title, imprisonment for up to 1 year, or both.

New section 3122—Applications

Proposed section 3122 of title 18 sets out the procedures for applying for a court order for a pen register or trap and trace device. Under subsection (a), a government attorney may apply for an order, or the extension of an order, authorizing or approving the installation and use of a pen register or trap and trace device. Such order must be made in writing under oath or affirmation to a court of competent jurisdiction.

Proposed paragraph 3122(a)(2) contains parallel provisions for state investigative or law enforcement officers. The phrase "Unless prohibited by state law," makes clear that this law does not preempt any existing state law regulating the installation and use of pen registers or trap and trace devices by state officials. To the extent that state law currently provides that a pen register or trap and trace device may only be installed or used by a state official based on some other, higher standard of proof, that law will continue in effect with respect to such officials.

Proposed subsection 3122(b) of title 18 sets out the contents required in an application for a court order for a pen register or a trap and trace device. The application must include the identity of the applicant and the law enforcement agency conducting the investigation. Also, the applicant must certify that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency.

New section 3123—Issuance of orders

Subsection (a) of proposed section 3123 provides that, upon application, a court shall issue an *ex parte* order authorizing the installation and use of a pen register or trap and trace device within its jurisdiction. To issue an order, the court must first be satisfied that the information sought is relevent to an ongoing criminal investigation. This provision does not envision an independent judicial review of whether the application meets the relevance standard, rather the court needs only to review the completeness of the certification submitted.

Proposed paragraph 3123(b)(1) describes the contents of the order authorizing the use or installation of a pen register or trap and trace device. The order shall specify (A) the identity, if known, of the person whose telephone line will receive the pen register; (B) the identity, if known, of the person who is under criminal investigation; (C) the number and, if known, location of the telephone line and, in the case of a trap and trace device, the geographic limits of the order; and (D) a statement of the offense to which the information likely to be obtained relates.

Under proposed paragraph 3123(b)(2), the order, upon request of the applicant, shall direct a third party to furnish information, facilities, and technical assistance necessary to install the pen register or trap and trace device. This provision of the order relating to cooperation is intended to codify the existing informal practice of cooperation between telephone companies and the Department of Justice.

Under proposed subsection 3123(c), the time period of authorization of installation and use of a pen register or a trap and trace device is 60 days, with possible extensions of 60 days. An extension may be granted upon application for a section 3122 order. The same judicial findings required by subsection 3123(a) are also required.

Proposed subsection 3123(d) provides that an order authorizing or approving the installation and use of a pen register or trap and trace device shall direct that the order be sealed, until otherwise ordered by the court. In addition, the order shall bar the disclosure of the existence of the pen register or trap and trace device and the disclosure of an investigation to the listed subscriber or to any other unauthorized person unless or until otherwise directed by the court. Intentional violations of the non-disclosure provisions may be, in appropriate circumstances, punishable as contempt.

New section 3124—Assistance in installation and use

Proposed subsection 3124(a) provides that upon the request of an authorized person, a wire or electronic communication service provider, landlord, custodian, or other person shall furnish such re-

quester with all information, facilities, and technical assistance necessary to effectuate the pen register order unobtrusively and with a minimum of interference. The Committee assumes that the current practice of law enforcement officials installing and maintaining pen registers will continue.

For trap and trace devices, proposed subsection 3124(b) provides that upon request of a government attorney or law enforcement officer authorized to receive the results, a wire or electronic communication service provider, landlord, custodian or other person shall promptly install the trap and trace device and furnish the requester all additional information, facilities and technical assistance, including installation and operation of the device unobtrusively and with a minimum of interference with services, provided that the installation and service is ordered under section 3123(b). This provision also requires that the results be furnished to the law enforcement officer designated by the court, at reasonable intervals, during regular business hours for the duration of the order, unless the court orders otherwise.

Proposed subsection 3124(c) provides reasonable compensation for those providing facilities and assistance under this section. This compensation provision is modeled after that which applies under section 2518 of title 18 and subsection 106(b) of this bill. It is intended to be interpreted and implemented in a similar fashion.

Proposed subsection 3124(d) provides that no cause of action shall lie in any court against a wire or electronic communication service provider, its officers, agents, employees or other specified persons for providing information, assistance or facilities in accordance with the terms of a chapter 206 court order.

Proposed subsection 3124(e) establishes a good faith defense against any civil or criminal action brought under chapter 206 or any other law.

New section 3125—Reports

Under a current order of the Attorney General, statistics concerning pen registers are compiled. Proposed section 3125 requires that this information be reformulated and submitted to the appropriate committees of Congress. It also extends such reporting requirements to trap and trace devices.

Specifically, proposed section 3125 requires that the Attorney General annually report to Congress on the number of pen register and trap and trace device orders applied for by law enforcement agencies of the Department of Justice. The Committee requests that these reports include information as to the nature of the offenses for which the pen registers and trap and trace devices are being used.

New section 3126—Definitions

Proposed section 3126 contains definitions for this chapter. The terms "wire communication," "electronic communication," and "electronic communication service" have the same meanings as in section 2510 of title 18. The term "court of competent jurisdiction" means (A) a district court of the United States (including a magistrate of such court) or a U.S. Court of Appeals; or (B) a state court

of general criminal jurisdiction authorized to enter pen register or trap and trace orders.

As indicated in proposed section 3126(3), the term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted for purposes of routing telephone calls, with respect to wire communications, on the telephone line to which such device is attached. Pen registers do not record the contents of a communication. They record only the telephone numbers dialed.

Devices used by a provider or customer or wire or electronic communication service incident to billing or cost accounting, or for any other similar purposes in the ordinary course of business are excluded from the definition of a pen register. Thus, devices that many companies and firms use to record billable time for their clients' accounts are outside this bill's prohibitions against the installation and use of pen registers.

Trap and trace devices are defined in proposed subsection 3126(4). A "trap and trace device" is a device which captures the incoming electronic or other impulses which identify the originating number of an incoming wire or electronic communication. Trap and trace devices do not record the contents of communications.

The term "attorney for the government" has the meaning given to that term by the Federal Rules of Criminal Procedure. The term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

Subsection 301(b) of the bill contains a clerical amendment to the table of chapters.

Section 302—Effective date

Section 302 of the bill contains the effective date for Title III of the Electronic Communications Privacy Act. Subsection (a) provides that as a general rule, Title III of the bill shall take effect 90 days after enactment. In the case of conduct pursuant to a court order or extension, these amendments apply only with respect to court orders or extensions made after this title takes effect. Subsection 302(b) of the bill contains special rules which, in essence, give states two years to bring their laws into conformity with the Electronic Communications Privacy Act's amendments to Federal law.

Section 303—Interference with the operation of a satellite

This section of the bill adds a new section to chapter 65 of title 18, United States Code.

New section 1367—Interference with the operation of a satellite

Subsection (a) of this proposed section provides that anyone who, without the authority of the satellite operator, intentionally or maliciously interferes with the authorized operation of a satellite or obstructs or hinders any satellite transmission, including both the transmission from the ground to the satellite and the transmission from the satellite to the ground (commonly known as the up-link and the down-link respectively) is subjected to criminal penalties including a fine of up to $250,000, imprisonment for not more than 10 years, or both. The subsection does not prohibit any actions by the authorized satellite operator which are designed to protect the satellite from unauthorized use.

Subsection (b) of this new section makes it clear that the criminal act described in subsection (a) does not include any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the United States. This subsection does not provide any new authority for such activities.

Finally, this section of the bill provides that the table of sections for chapter 65 of title 18 is amended to include the new section 1367.

VI. Agency Views

On June 25, 1986 and July 29, 1986, the Committee received the following letters from the Department of Justice.

U.S. Department of Justice,
Office of Legislative and Intergovernmental Affairs,
Washington, DC, June 25, 1986.

Hon. Strom Thurmond,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

Dear Mr. Chairman: This letter is to advise you of the Department of Justice's position with regard to S. 2575, the Electronic Communications Privacy Act of 1986. This bill, which is identical to H.R. 4952 as recently passed by the House of Representatives, makes important changes to the existing wiretap statutes and fills gaps in current laws by creating provisions to regulate interception of and access to new forms of electronic communication such as data transmissions.

The Department of Justice has worked intensively on this legislation over the past several weeks with the staff of the Subcommittee on Patents, Copyrights and Trademarks, as well as with interested representatives of industry and civil liberties groups. While initial versions of this legislation did not in our view adequately safeguard legitimate and vital law enforcement and national security needs for access to communications, as a result of the negotiations that have occurred the bill has been substantially modified to accommodate our concerns. In our judgment the bill as presently drafted fairly balances the interests of privacy and law enforcement and its enactment would represent a major accomplishment of the 99th Congress, holding forth the promise of significant benefits for business, privacy, and law enforcement alike.

Accordingly, the Department of Justice strongly supports the enactment of S. 2575.

Sincerely,

John R. Bolton,
Assistant Attorney General.

U.S. Department of Justice,
Office of Legislative and Intergovernmental Affairs,
Washington, DC, 20530 July 29, 1986.

Hon. Strom Thurmond,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

Dear Mr. Chairman: This is with further reference to my letter of June 25, 1986, expressing support for S. 2575, the Electronic Communications Privacy Act of 1986. A copy of my earlier letter is enclosed for ready reference.

We continue to believe that this measure is a well balanced one which, in addition to modernizing the 1968 electronic surveillance law, also benefits both law enforcement and individual privacy by clarifying many aspects of this highly complex area of the law. As the 99th Congress is rapidly drawing to a close, we sincerely hope that the Senate will act on S. 2575 at an early date.

We would deeply appreciate your consideration of S. 2575 and, if possible, your formal co-sponsorship of the bill. Having your name on the bill would, we believe, be most helpful in efforts to process this important legislation this year.

Sincerely,

John R. Bolton,
Assistant Attorney General.

VII. Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, September 23, 1986.

Hon. Strom Thurmond,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has reviewed S. 2575, the Electronic Communications Privacy Act of 1986, as ordered reported by the Senate Committee on the Judiciary, September 19, 1986. CBO estimates that enactment of this legislation would result in no significant cost to the federal government and in no cost to state or local governments.

S. 2575 would make a number of amendments to Title 18 of the U.S. Code concerning access to electric communications. Title I of the bill would establish penalties for the unlawful interception or disclosure of electronic communications, provide for the recovery of civil damages for persons whose communications are intercepted, disclosed or used in violation of this provision, and modify procedures for government interception of communications. Title II would create specific penalties for unlawful access to stored wire and electronic communications, while Title III would establish a general prohibition on the use of pen registers. These titles would mandate specific procedures for access to stored communications and use of pen registers by government entities, and Title II would allow for civil actions.

S. 2575 would require government entities to compensate private parties assembling or providing information concerning stored electronic communications, or assisting in the installation and use of a pen register. Because such compensation is currently provided in Department of Justice (DOJ) investigations, CBO does not expect the these provisions would result in any significant additional cost to the federal government.

Based on information from the DOJ, we do not expect that enactment of this bill would result in a significant change in the government's law enforcement practices or expenditures. S. 2575 would specifically authorize law enforcement efforts the DOJ is currently undertaking with other authority.

If you wish further details on this estimate, we will be pleased to provide them.

With best wishes,

Sincerely,

James Blum
(for Rudolph G. Penner, Director).

VIII. Regulatory Impact Statement

In compliance with paragraph 11(b) of Rule XXVI of the Standing Rules of the Senate, the Committee has concluded that no significant additional regulatory impact would be incurred in carrying out the provisions of this legislation. After due consideration, the Committee concluded that the changes in existing law contained in the bill will not increase or diminish any present regulatory responsibilities of the U.S. Department of Justice or any other department or agency affected by the legislation.

IX. Vote of Committee

On August 12, 1986, the Subcommittee on Patents, Copyrights, and Trademarks, with a quorum present, reported S. 2575, with an amendment in the nature of a substitute, to the Committee on the Judiciary by voice vote. On September 19, 1986, the Judiciary Committee adopted two further changes in the bill as reported by the Subcommittee. The Judiciary Committee, with a quorum present, and without objection heard, approved the amendment in the nature of a substitute. The Committee then favorably reported S. 2575, as amended, by unanimous consent.

X. Changes in Existing Law

In compliance with paragraph 12 of Rule XXVI, of the Standing Rules of the Senate, changes in existing law made by S. 2575 as reported are shown as follows (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 18—CRIMES AND CRIMINAL PROCEDURE

PART I. CRIMES

PART II—CRIMINAL PROCEDURE

CHAPTER 65—MALICIOUS MISCHIEF

§ 1367. Interference with the operation of a satellite

(a) Whoever, without the authority of the satellite operator, intentionally or maliciously interferes with the authorized operation of a communications or weather satellite or obstructs or hinders any satellite transmission shall be fined in accordance with this title or imprisoned not more than ten years of both.

(b) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency or of an intelligence agency of the United States.

* * * * * * *

CHAPTER 109—SEARCHES AND SEIZURES

* * * * * * *

§ 2232. Destruction or removal of property to prevent seizure

(a) Physical Interference With Search.—Whoever, before during, or after seizure of any property by any person authorized to make searches and seizures, in order to prevent the seizure or securing of any goods, wares, or merchandise by such person, staves, breaks, throws overboard, destroys, or removes the same, shall be fined not more than $10,000 or imprisoned more than five years, or both.

(b) Notice of Search.—Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise or other property, gives notice or attempts to give notice of the possible search or seizure to any person shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(c) Notice of Certain Electronic Surveillance.—Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both.

Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years, or both.

* * * * * * *

CHAPTER 119—WIRE *AND ELECTRONIC COMMUNICATIONS* INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

§ 2510. Definitions

As used in this chapter—

(1) "wire communication" means any [communication] *aural transfer* made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception *(including the use of such con-*

nection in a switching station) furnished or operated by any person engaged [as a common carrier] in providing or operating such facilities for the transmission of interstate or foreign communications *or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit*.

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, *but such term does not include any electronic communication;*

* * * * * * *

(4) "intercept" means the aural *or other* acquisition of the contents of any wire, *electronic*, or oral communication through the use of any electronic, mechanical, or other device.

(5) "electronic mechanical, or other device" means any device or apparatus which can be used to intercept a wire [or oral], *oral, or electronic* communication other than—

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a [communications common carrier] *provider of wire or electronic communication service* in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business *or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business*; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

* * * * * * *

(8) "contents", when used with respect to any wire [or oral], *oral, or electronic* communication, includes any information concerning the [identity of the parties to such communication or the existence,] substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means—

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire [or oral], *oral, or electronic* communications;

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of title 47 of the United States Code; [and]

(11) "aggrieved person" means a person who was a party to any intercepted wire [or oral], *oral, or electronic* communication or a person against whom the interception was directed[.]*;*

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

(B) any wire or oral communication;

(C) any communication made through a tone-only paging device; or

(D) any communication from a tracking device (as defined in section 3117 of this title);

(13) "user" means any person or entity who—

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not—

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

§ 2511. Interception and disclosure of wire or oral communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

(a) [willfully] *intentionally* intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire [or oral] *oral, or electronic* communication;

(b) [willfully] *intentionally* uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication, or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) [willfully] *intentionally* discloses, or endeavors to disclose, to any other person the contents of any wire [or oral] *oral, or electronic* communication, knowing or have reason to know that the information was obtained through the interception of a wire [or oral] *oral, or electronic* communication in violation of this subsection; or

(d) [willfully] *intentionally* uses, or endeavors to use, the contents of any wire [or oral] *oral, or electronic* communication, knowing or having reason to know that the information was obtained through the interception of a wire [or oral] *oral, or electronic* communication in violation of this subsection; [shall be fined not more than $10,000 or imprisoned not more than five years, or both.] *shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).*

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of [any communication common carrier,] *a provider of wire or electronic com-*

munication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property [of the carrier of such communication: *Provided*, That said communication common carriers] *of the provider of that service, except that a provider of wire communication service to the public* shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, *providers of wire or electronic communication service*, [communication common carriers,] their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire [or oral], *oral, or electronic* communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if [the common carrier,] *such provider* its officers, employees, or agents, landlord, custodian, or other specified person has been provided with—

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No [communication common carrier] *provider of wire or electronic communication service* officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished an order or certification under this subparagraph, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any [violation of this subparagraph by a communication common carrier or an officer, employee, or agent thereof] *such disclosure*, shall render [the carrier] *such person* liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any [communication common carrier] *provider of wire or electronic communication service* its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of [an order of certification under this subparagraph] *a court order or certification under this chapter*.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforce-

ment of chapter 5 of title 57 of the United States Code, to intercept a wire or *electronic* communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire [or oral], *oral, or electronic* communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire [or oral], *oral, or electronic*, communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State [or for the purpose of committing any other injurious act].

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an office, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or *chapter 121*, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communication [by], *or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing* a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress.

(II) by any governmental, law enforcement, civil defense private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

(I) is prohibited by section 633 of the Communications Act of 1934, or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter—

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire a electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(3)(a) Except as provided in paragraph (b) of this subsection a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five year, or both.

(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the

offense under paragraph (a) is a radio communication that is not scrambled or encrypted, then—

(i) If the communication is not the radio portion of a cellular telephone communication, a public land mobile radio service communication or a paging service communication, and them conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both, and

(ii) if the communication is the radio portion of a cellular telephone communication, a public land mobile radio service communication or a paging service communication, the offender shall be fined not more than 500

(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted—

((i) to a brodcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)(a)(i) If the communication is—

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection—

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

§ 2512. Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who [willfully] *intentionally*—

(a) sends through the mail, or sends or carriers in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications;

(b) manufacturers, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication any advertisement of—

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications,

knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for—

(a) [a communications common carrier] *a provider of wire or electronic communication service* or an officer, agent, or employee of, or a person under contract with, [a communications common carrier] *such a provider*, in the normal course of the [communications common carrier's business] *business of providing that wire or electronic communication service*, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications.

§ 2513. Confiscation of wire [or oral], *oral, or electronic* communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose of the Attorney General.

§ 2515. Prohibition of use as evidence of intercepted wire [or oral], *oral, or electronic* communications

Whenever any wire [or oral], *oral, or electronic* communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

§ 2516. Authorization for interception of wire [or oral], *oral, or electronic* communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, [or] any Assistant Attorney General, *any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division* specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire of oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of

the Atomic Energy Act of 1954), *section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel)*, or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), [or] chapter 192 (relating to riots), *chapter 65 (relating to malicious matter mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy)*;

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murders, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 224 (bridery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1084 (transmission of wagering information), *section 751 (relating to escape)*, sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transporation in aid of racketeering enterprises), section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity), section 1954 (offer acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 2252 or 2253 (sexual exploitation of children), Section 2251 and 2252 (sexual exploitation of children), section [2314] *2312, 2313, 2314*, and 2315 (interstate transportation of stolen property), *the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities)*, section 1963 violations with respect to racketeer influenced and corrupt organizations), *section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud)*, [or] section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassination, kidnapping, and assault), *section 831 (relating to prohibited transaction involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), or section 1992 (relating to wrecking trains)*;

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions); [or]

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any violation of section 1679(c)(2) (relating to destruction of a natural gas pipeline) or subsection (i) or (n) of the United States Code;

(j) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act); or

(k) the location of any fugitive from justice from an offense described in this section; or

[(h)] *(l)* any conspiracy to commit any of the foregoing offenses.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire [or oral], *oral, or electronic* communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire [or oral], *oral, or electronic* communications by investigative or law enforcement of officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

§ 2517. Authorization for disclosure and use of intercepted wire [or oral], *oral, or electronic* communication

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire [or oral], *oral, or electronic* communication,

or evidence derived therefrom may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire [or oral], *oral, or electronic* communication or evidence derived therefrom any use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire [or oral], *oral, or electronic* communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire [or oral], *oral, or electronic* communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized herein, intercepts wire [or oral], *oral, or electronic* communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

§ 2518. Procedure for interception of wire [or oral], *oral, or electronic* communications

(1) Each application for an order authorizing or approving the interception of a wire [or oral], *oral, or electronic* communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) *except as provided in subsection (11),* a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought

to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire [or oral], *oral, or electronic* communications involving any of the same persons, facilities or places specified in the application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire [or oral], *oral, or electronic* communications within the territorial jurisdiction of the court in which the judge is sitting *(and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction)* if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter.

(b) there is probable cause for brief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) *except as provided in subsection (11),* there is probable cause for belief that the facilities from which, or the place where the wire [or oral], *oral, or electronic* communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire [or oral], *oral, or electronic* communication under this chapter shall specify—

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire [or oral], *oral, or electronic* communication under this chapter shall, upon request of the applicant, direct that a [communication common carrier], *provider of wire or electronic communication service,* landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such [carrier] *service provider,* landlord, custodian, or person is according the person whose communications are to be intercepted. Any [communication common carrier] provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant [at the prevailing rates.] *for reasonable express incurred in providing such facilities or assistance.*

(5) No order entered under this section may authorize or approve the interception of any wire [or oral], *oral, or electronic* communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. *Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered.* Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise, subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. *In the event the intercepted communications is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Goverment personnel, or by an individual operating under a contract with the Government,*

acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant of that State, who reasonably determines that—

(a) an emergency situation exists that involves—

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire [or oral], *oral, or electronic* communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception.

may intercept such wire [or oral], *oral, or electronic* communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire [or oral], *oral, or electronic* communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)(a) The contents of any wire [or oral], *oral, or electronic* communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire [or oral], *oral, or electronic* communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under this directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire [or oral], *oral, or electronic* communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire [or oral], *oral, or electronic* communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire [or oral], *oral, or electronic* communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less then ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of the section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

(a) in the case of an application with respect to the interception of an oral communication—

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

(b) in the case of an application with respect to a wire or electronic communication—

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

(iii) the judge finds that such purpose has been adequately shown.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

§ 2519. Reports concerning intercepted wire [or oral], *oral, or electronic* communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for *(including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of title)*;

(c) the fact that the order or extension was granted as applied for, was modified, or was denied,

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension or an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire [or oral], *oral, or electronic* communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

§ 2520. Recovery of civil damages authorized

[Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person—

[(a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

[(b) punitive damages; and

[(c) a reasonable attorney's fee and other litigation costs reasonably incurred.

A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or under any other law.]

(a) IN GENERAL.—Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) RELIEF.—In an action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate,

(2) damages under subsection (c) and punitive damages in appropriate cases, and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) COMPUTATION OF DAMAGES.—(1) In an action under this section, if the conduct is in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1,000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of—

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) DEFENSE.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

§ 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon a practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons

for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the federal Rules of Criminal Procedure.

*   *   *   *   *   *   *

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Sec.

§ 2701. Unlawful access to stored communications

(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—

(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.

(c) EXCEPTIONS.—Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

§ 2702. Disclosure of contents

(a) PROHIBITIONS.—Except as provided in subsection (b)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(b) EXCEPTIONS.—A person or entity may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2516, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

(6) to a law enforcement agency, if such contents—

(A) were inadvertently obtained by the service provider; and

(B) appear to pertain to the commission of a crime.

§ 2703. Requirements for governmental access

(a) CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) CONTENTS OF ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any

electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1)(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

(B) A provider or electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity—

(i) uses an administrative subpoenal authorized by a Federal or State statute, or a Federal or State grand jury subpoena;

(ii) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant;

(iii) obtains a court order for such disclosure under subsection (d) of this section; or

(iv) has the consent of the subscriber or customer to such disclosure.

(2) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer

(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) of this section shall issue only if the governmental entity shows that there is reason to believe the con-

tents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No Cause of Action Against a Provider Disclosing Information Under This Chapter.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under this chapter.

§ 2704. Backup preservation

(a) Backup Preservation.—(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of—

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider—

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the governmental entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

(b) Customer Challenges.—(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement—

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

§ 2705. Delayed notice

(a) Delay of Notification.—(1) A governmental entity acting under section 2703(b) of this title may—

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is—

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that—

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber—

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of Notice to Subject of Governmental Access.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

(1) endangering the life or physical safety or an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

§ 2706. Cost reimbursement

(a) Payment.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) Amount.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

§ 2707. Civil action

(a) Cause of Action.—Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or

entity which engaged in that violation such relief as may be appropriate.

(b) Relief.—In a civil action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

(d) Defense.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

(e) Limitation.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

§ 2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) Duty to Provide.—A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required Certification.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the wire or electronic communication service provider to which the request is made that—

(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(c) Prohibition of Certain Disclosure.—No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) Dissemination by Bureau.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement That Certain Congressional Bodies Be Informed.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

§ 2710. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

* * * * * * *

CHAPTER 205—SEARCHES AND SEIZURES

§ 3117. Mobile tracking devices

(a) In General.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

(b) Definition.—As used in this section, the term "tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or object.

CHAPTER 206—PEN REGISTERS AND TRAP AND TRACE DEVICES

§ 3121. General prohibition on pen register and trap and trace device use; exception

(a) In General.—Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) Exception.—The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service—

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse or service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service, or with the consent of the user of that service.

(c) Penalty.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

§ 3122. Application for an order for a pen register or a trap and trace device

(a) Application.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) Contents of Application.—An application under subsection (a) of this section shall include—

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

§ 3123. Issuance of an order for a pen register or a trap and trace device

(a) In General.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device

within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(b) Contents of Order.—An order issued under this section—

(1) shall specify—

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the number and, if know, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and

(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

(c) Time Period and Extensions.—(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.

(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

(d) Nondisclosure of Existence of Pen Register or a Trap and Trace Device.—An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that—

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line to which the pen register or a trap and device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

§ 3124. Assistance in installation and use of a pen register or a trap and trace device

(a) Pen Registers.—Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively

and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

(b) TRAP AND TRACE DEVICE.—Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the officer of a law enforcement agency, designated in the court, at reasonable intervals during regular business hours for the duration of the order.

(c) COMPENSATION.—A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonble expenses incurred in providing such facilities and assistance.

(d) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order under this chapter.

(e) DEFENSE.—A good faith reliance on a court order, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

§ 3125. Reports concerning pen registers and trap and trace devices

The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice.

§ 3126. Definitions for chapter

As used in this chapter—

(1) the terms 'wire communication', 'electronic communication', and 'electronic communication service' have the meanings set forth for such terms in section 2510 of this title;

(2) the term 'court of competent jurisdiction' means—

(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

(3) the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

(4) the term 'trap and trace device' means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted;

(5) the term 'attorney for the Government' has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

(6) the term 'State' means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

O

Memorandum

FDH:mkf:tmb

Subject	Date
The Electronic Communications Privacy Act of 1986	DEC 15 1986

To
All United States Attorneys
and Strike Force Chiefs

From
William F. Weld
Assistant Attorney General
Criminal Division

Public Law 99-508, the Electronic Communications Privacy Act of 1986, was signed into law on October 21, 1986 by President Reagan. It is the most far reaching revision of the law on electronic surveillance enacted since passage of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Attached is a memorandum describing the new Act with emphasis on its effect on existing federal law and practice as well as a copy of the statute.

Most of the features of the Electronic Communications Privacy Act go into effect 90 days after enactment which will occur on January 20, 1987. It is important that each federal prosecutor become fully aware of its provisions, many of which are beneficial to law enforcement interests. In summary, these are the highlights of the legislation, all of which are more fully discussed in the attached descriptive memorandum:

- - maintaining the current basic definitions of wire and oral communications thus preserving 18 years of legal precedent;

- - creating statutory coverage for a wide range of communications within the defined term "electronic communications" that will include non-aural communications such as electronic mail, computer transmissions and video teleconferencing;

- - requiring court orders for government interception of electronic communications and providing criminal sanctions for third party interceptions;

- - including cellular telephone communications and digital display and voice pagers within the coverage of the statute and excluding handheld or cordless telephones, tone only beepers and tracking devices from the statute;

- - permitting a form of "roving tap" that will enable law enforcement officers to target a person and intercept his oral, wire or electronic communications without the need to specify the exact location or telephone in advance in the court order;

- - establishing a statutory method governing government access to stored electronic communications, such as copies of electronic mail held by a service provider or computer data held by a third party data processing company;

- - creating a statutory court order or subpoena requirement for government access to telephone toll records based on a standard of relevance to an ongoing law enforcement investigation;

- - creating a statutory requirement of a court order for government access to pen register and trap and trace data based on a standard of relevance to an ongoing law enforcement investigation and basically following existing Department of Justice practice;

- - permitting ordinary government personnel or contract employees to monitor ongoing electronic surveillance under the direction of law enforcement personnel;

- - permitting after the fact minimization in the case of foreign languages or coded conversations where translators are not readily available;

- - increasing the number of predicate offenses for oral or wire interceptions by several dozen specific felonies;

- - permitting interception of electronic communications based on any federal felony;

- - permitting authorization of electronic communication interceptions by a law enforcement official in the field instead of requiring Washington approval; however, for the first three years Washington approval will be required; and

- - allowing up to ten days to install an oral, wire or electronic communications interception device prior to the start of the 30 day interception period.

The above list reflects but a few of the more important changes and innovations set forth in the Act and described in the attached memorandum. I urge you and your staff to study the memorandum and the Act carefully. An even fuller description of the Act and its provisions and policy implications will be forthcoming in the future in a full revision of Chapter 7 of Title 9 of the United States Attorneys' Manual. In addition, draft applications, orders and other pleadings will be prepared and distributed for a number of the requirements of the Act.

Any questions you have on this subject should be directed to the Office of Enforcement Operations in the Criminal Division. FTS: 633-3684 or 633-2869

Attachment

ANALYSIS OF THE ELECTRONIC
COMMUNICATIONS PRIVACY ACT OF 1986,
PUBLIC LAW NO. 99-508

Prepared by the Office of Enforcement Operations, Criminal Division, United States Department of Justice

DEC 15 1986

On October 21, 1986, President Reagan signed into law the Electronic Communications Privacy Act of 1986, Public Law No. 99-508. This legislation is primarily a comprehensive revision of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. It provides coverage for the technological advances developed in the area of electronic communications since the passage of the original act. The 1968 act governed only the aural acquisition of the contents of a wire or oral communication. Thus, if the intercepted conversation could not be heard or understood by the human ear, the existing law did not apply. The new legislation encompasses not only the interception of wire and oral communications as defined in the original act, but virtually all forms of non-aural electronic communications during both the transmission stage and the period when such communications are maintained in electronic storage. Included within the concept of electronic communication are such new and increasingly utilized communication methods as electronic mail, computer data transmissions and video teleconferencing. The principal purpose of the new statute is to regulate the use of these dramatically improved communications technologies that have been developed since 1968 and to protect the transmission of all forms of information, including voice, data and some forms of video, from improper interception. The overall thrust of the legislation is to expand privacy protection in the new areas of electronic communication while recognizing and preserving the interests of effective law enforcement. The purpose of this memorandum is to provide a broad overview of the new Act and acquaint you with those provisions that have special significance for federal law enforcement.

Initially, it should be noted that most of the provisions of the new Act become effective on January 20, 1987, which is 90 days from the date the Act was signed. There is, however, one provision of the Act which takes effect immediately. The new provisions of 18 U.S.C. 2516 extend authority to authorize a request for an electronic surveillance order to any Acting Assistant Attorney General or Deputy Assistant Attorney General in the Criminal Division, as well as to an Assistant Attorney General, once those officials are so designated by the Attorney General. This provision of the Act will be implemented by a new Attorney General delegation order.

It should also be noted at the outset that while the intent of the new statute is to cover all known electronic communications technologies to which an expectation of privacy can reasonably attach, several exceptions were made to exclude forms of communications where privacy interests were deemed to be relatively weak (e.g., handheld or cordless telephones, tone only pagers) or nonexistent (e.g., many forms of radio communications). These exceptions will be discussed in detail later in this memorandum.

The Electronic Communications Privacy Act of 1986 is divided into three separate, but closely related, titles: Title I - Interception of Communications and Related Matters; Title II - Stored Wire and Electronic Communications and Transactional Records Access; and Title III - Pen Registers and Trap and Trace Devices.

TITLE I-THE INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

The first portion of the new Act is comprised of amendments to Title III of the 1968 act. The amendments establish a new category denominated "electronic communications" in addition to the wire and oral communications covered under the original act and address some of the difficulties perceived by law enforcement officials in utilizing the former Title III. 18 U.S.C. 2510-2520.

The new statute defines and regulates three types of communications: (1) wire; (2) oral; and (3) electronic communications. The last type, in essence, is any form of communication using electronics in which the human voice is not utilized. In addition, in one transmission there may be more than one type of communication, such as a voice telephone conversation followed by a computer transmission on the same line utilizing modems. All forms of communications will now be covered with the limited exceptions noted below. Thus, coverage of transmission of electronic communications both from the perspective of protecting the individual communication from third party interception and regulating governmental interception will be virtually all-inclusive.

In actuality, the new Act mandates little change in the substantive or procedural requirements for obtaining an order to intercept a traditional wire or oral communication. For the most part, with respect to wire and oral communications, the United States Attorneys will proceed in precisely the same manner as they have in the past. With respect to electronic communications, the substantive provisions of the law are primarily the same as those governing oral and wire communications, but the procedural provisions are somewhat different. The Act treats electronic communications in two different categories. Title I of the Act regulates interception of electronic communications during the transmission stage and, accordingly, treats them much as a wire or oral interception, although, as noted, with several lessened procedural requirements. Title II of the Act, discussed infra, is directed to electronic records that are temporarily in storage before or

after the actual transmission. Many of the changes to the wire or oral communications provisions noted below are quite beneficial to law enforcement, and many of these were made at the Department's suggestion.

The new Act's most significant changes, additions and exceptions set forth in Title I are the following:

(1) Wire Communications

The definition of "wire communication" under the old statute has been redrafted to include only "aural transfers," which are defined as communications that involve the human voice at some point in the transmission. 18 U.S.C. 2510(1)(18). Wire communications are specifically excluded from the new definition of electronic communications. 18 U.S.C. 2510(12)(B). The Department insisted on keeping the distinction between wire and electronic communications in order to ensure that the case law in this area, built up over 18 years, would continue to be applicable and the courts would not be called upon to reinterpret established electronic surveillance principles.

The new law eliminates the distinction contained in the original Title III between common carrier and non-common carrier electronic communication systems where the system is designed to carry private communications not readily accessible to the public. The new Act applies to any person (as defined in 18 U.S.C. 2510(6)) engaged in providing facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce. 18 U.S.C. 2510(1). This amendment was added to provide coverage of private communications systems where the affecting commerce jurisdictional basis is present. This change is in recognition of the fact that some major corporations and professional firms that are not traditional common carriers are installing their own private communications systems.

(2) Oral Communications

The definition of oral communication remains the same but is specifically excluded from the definition of electronic communication. 18 U.S.C. Section 2510(2). The effect of the exclusion is to make it clear that an oral communication under the statute can never be a radio communication. See, United States v. Rose, 669 F.2d 23, 25-26 (1st Cir.) cert. denied, 459 U.S. 828 (1982)

(3) Electronic Communications

An "electronic communication" under the new statute is any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system that affects interstate or foreign commerce. "Electronic communication" is also specifically defined to exclude a wire or oral communication. 18 U.S.C. 2510(12)(B). The effect of the breadth of this definition is that any and all forms of electronic communications, unless specifically exempted, are now subject to the provisions of the statute just as wire communications have been covered since 1968.

The term "intercept" under the new Act has been broadened to mean the aural "or other" acquisition of the contents of wire, electronic or oral communications. The "or other" was added to accommodate the non-aural acquisition of electronic communications. 18 U.S.C. 2510(4)

(4) Exceptions

Because the definition of electronic communication is so broad and all-inclusive it became necessary to carve out some forms of electronic communications that either appeared patently not to be deserving of privacy protection or where a policy decision was made by the Congress not to include a specific form of electronic communication. Those exceptions appear in the legislation either as exceptions to defined terms in 18 U.S.C. 2510 or as exceptions to the section that penalizes certain activity as unlawful, 18 U.S.C. 2511. The exceptions are as follows:

(a) The radio portion of handheld or cordless telephone conversations. These utilize a radio transmission over a limited distance to a base station at a regular telephone. They are so easily intercepted, often over an ordinary AM radio, that the decision was made that there is no reasonable expectation of privacy in these communications. Such handheld, cordless, telephones should be distinguished from cellular telephones, which are covered under the Act. 18 U.S.C. 2510(12)(A)

(b) Tone only paging devices. It has been the Department's position that intercepting only tone beeps or vibrations from a pager is not a search and, therefore, such interceptions raise no Fourth Amendment implications; the Act endorses this policy. By contrast, digital display and voice paging devices are covered by the new legislation. 18 U.S.C. 2510(12)(C)

(c) Communications from tracking devices (beepers) placed in automobiles or packages to trace their location. 18 U.S.C. 2510(12)(D). These are specifically excluded from this legislation because of the manner in which they function and the limited privacy implications related to their use. This area is being left to case law development. However, the new legislation adds a new 18 U.S.C. 3117 to specifically solve one problem that arises in the use of

mobile tracking devices. These devices, by their nature, can easily be transported across jurisdictional lines. However, a court order, in those circumstances where one is required under case law, might well be limited to one judicial district. This new section provides extra-jurisdictional effect to a court order that authorizes the installation of a mobile tracking device. It should be noted that the authorization outside the jurisdiction of the court is not limited to the territorial jurisdiction of the United States for a mobile tracking device.

(d) A partial exception for video interceptions exists. The new Act covers and criminalizes the unauthorized interception of a closed circuit television broadcast between two points. For example, a business competitor breaking into the wire transmission of a teleconference violates the law, and a law enforcement interception of that communication by tapping into the lines requires a court order under the statute. The Act, however, does not cover the government's use of its own video equipment to surreptitiously intercept and televise a meeting without the consent of a party because there is no interception of an electronic communication occurring as no wires are tapped. (See H. Rep. No. 99-647, 99th Cong., 2d Sess. p. 36 (1986)) The latter does require a search warrant issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure and, accordingly, the law in this area has been left to the courts to develop. See, United States v. Biasucci, 786 F.2d 506 (2nd Cir. 1986); United States v. Torres, 751 F.2d 875 (7th Cir. 1984), cert. denied, 105 S. Ct. 1853 (1985).

(e) Pen registers and trap and trace devices. These investigative tools qualify as electronic communications as that term is broadly defined. Since the privacy interests involved are so limited with these techniques, they have both been excluded from the coverage of Title I of the Act. 18 U.S.C. 2511(h)(i). However, Title III of the Act specifically regulates these techniques. By and large that Title, to be discussed infra, merely codifies existing Department policy and practices on pen registers and trap and trace devices. 18 U.S.C. 3121 - 3125.

(f) Certain radio communications. The definition of electronic communication is so broad that it sweeps in all forms of radio communications. Thus, it was necessary for the statute to specifically exclude various forms of radio communications that patently should not be subject to protection from interception such as electronic communications that are broadcast so as to be readily accessible to the public (AM and FM radio station broadcasts), ship to shore general public type communications, public safety communications, citizen band radio, general mobile radio services and the like. 18 U.S.C. 2511(2)(g). This subsection of the Act also contains other specific exceptions relating to interaction with the Federal Communications Act or where there is a necessity to service the system or locate interference. Id.

(5) Hybrid Communications

To cure the ambiguities that exist relating to conversations that are in part wire and in part radio communications, the Act had to address handheld or cordless telephone conversations, cellular telephone conversations and paging devices. All of these combine wire and electronic communications. See, United States v. Hall, 488 F.2d 193 (9th Cir. 1973). As noted, the radio portion of a handheld or cordless telephone communication is specifically excluded from the Act. 18 U.S.C. 2510(1). This is in recognition of the fact that such "backyard" phones are so easily intercepted within their very short range from the base station phone that no true privacy interests can be deemed present. An interception of the wire portion of such a conversation, however, is covered by the Act as long as the interception is made on the wire portion as opposed to listening to the radio portion.

Both the wire and radio portions of a cellular telephone conversation are specifically covered by the Act. A reference to connections in switching stations in 18 U.S.C. 2510(1) is included so that even radio to radio cellular communications that would occur in a conversation between persons utilizing two cellular car phones will come within the proscriptions of the statute. Including cellular communications within the statute is a Congressional recognition that persons using car phones or briefcase phones that are fully mobile expect that their conversations are private, much as conversations on traditional telephones are private. The mobility of these phones, as opposed to the very limited mobility of a handheld, cordless phone, and the difficulty of intercepting cellular conversations also argue for their privacy protection.

Another problem addressed by the statute is the potential for combining both wire and electronic communications into one conversation over the same telephone line. For instance, two parties can converse in a normal voice conversation, then, using modems, send data to computer terminals and/or exchange written messages on their terminals, and later return to the voice communication method before terminating the conversation. The legislative history makes it clear that if any part of the conversation is a wire communication, then for purposes of the statute, Congress expects that the conversation will be deemed a wire communication. H. Rep. No. 99-647, supra, at p. 35. This has only a limited practical effect because only certain of the

procedural aspects of the statute are different for wire communications than they are for electronic communications.

(6) Penalties

The basic penalty provisions of the existing statute are retained and anyone who intentionally discloses or endeavors to disclose the contents of any wire, oral or electronic communication having reason to know the information was obtained through an unlawful interception is subject to both criminal and civil penalties. Thus, the penalty provisions that apply to the illegal tapping of wire communications are extended to interceptions of electronic communications.

Several of the existing penalty provisions have been modified. For instance, the culpability standard for all wire, oral or electronic communications interception offenses has been changed from "willfully" to "intentionally." 18 U.S.C. 2511. Initial research indicates that this change will be of little practical effect.

In addition, the penalty provision for the interception of the radio portion of a cellular telephone conversation required careful handling because of the presence of radio scanners on the market. These scanners, which are currently in the hands of amateur radio hobbyists, are designed so that they can intercept cellular calls as long as the cellular phone and the radio interceptee are in the same cell and on the same frequency. A first offense for such an interception, if the interception is not for a tortious or illegal purpose or for commercial gain, carries only a $500 fine. 18 U.S.C. 2511(4)(b)(ii). Subsequent offenses or an offense for a tortious or illegal purpose or for commercial gain can carry up to a five year prison term. 18 U.S.C. 2511(4)(a).

Finally, the bill also sets up a reduced penalty structure for a private home television viewer who, using a satellite dish, intercepts specified unscrambled satellite transmissions for private, non-commercial use. For a first offense under these circumstances the only sanction available will be a civil suit by the federal government seeking injunctive relief. 18 U.S.C. 2511(5)(a)(ii).

A full discussion of the penalty provisions of the statute will appear later in an amended United States Attorneys' Manual section.

The legislation also adds a new provision to Title 18 that criminalizes the disclosure of a court approved electronic surveillance application. This new statute, added as a subsection (c) to 18 U.S.C. 2232, provides a five year penalty and a fine for warning, or attempting to warn, the subject of an electronic surveillance application "in order to obstruct, impede, or prevent such interception." The provision applies to both interceptions under the new Act and those authorized under the Foreign Intelligence Surveillance Act (50 U.S.C. 1801, et seq.). Disclosure of existing wiretap orders has been an occasional problem in recent years, since not all cases fit within the less specific obstruction of justice and contempt statutes. A specific offense will close this gap.

(7) New Crimes

A large number of new crimes have been added to the list of crimes enumerated in 18 U.S.C. Section 2516 for which a wire or oral interception order can be obtained. Expansion of the list of wiretap predicate offenses was a major goal of the Department in the drafting of the Act and should work to make this investigative technique more useful. These additional crimes are: 18 U.S.C. 751 (escape), 18 U.S.C. 1952A (use of interstate commerce facilities in the commission of murder for hire), 18 U.S.C. 1952B (violent crimes in aid of racketeering activity), 18 U.S.C. 2312, 2313, 2314, (interstate transportation or receipt of stolen vehicles), the second section 2320 of Title 18 (trafficking in certain motor vehicles or motor vehicle parts), 18 U.S.C. 1203 (hostage taking), 18 U.S.C. 1029 (fraud and related activity in connection with access devices), 18 U.S.C. 3146 (penalty for failure to appear), 18 U.S.C. 3521(b)(3) (witness relocation and assistance), 18 U.S.C. 32 (destruction of aircraft or aircraft facilities), 18 U.S.C. 115 (threatening or retaliating against a federal official), 18 U.S.C. 1365 (destruction of an energy facility), 18 U.S.C. 1341 (mail fraud), 18 U.S.C. 2511, 2512 (interception and disclosure of certain communications and use of certain interception devices), 18 U.S.C. 831 (prohibited transactions involving nuclear materials), 18 U.S.C. 33 (destruction of motor vehicles or motor vehicle facilities), 18 U.S.C. 1992 (wrecking trains), 22 U.S.C. 2778 (relating to the Arms Export Control Act), 42 U.S.C. 2284 (sabotage of nuclear facilities or fuel), 49 U.S.C. 1679(c)(2) (destruction of natural gas pipeline), 49 U.S.C. 1472(i) or (n)(aircraft piracy), and any felony violations of Chapter 65 (malicious mischief), Chapter 111 (destruction of vessels), and Chapter 81 (piracy) of Title 18, United States Code. In addition, a new subsection was added that authorizes interception to ascertain the location of any fugitive from justice from an offense described in 18 U.S.C. 2516(1).

(8) Procedural Changes

Section 2518 of Title 18, which describes the procedure for intercepting wire, oral, and now electronic communications remains substantially the same under the new law. There are, however, some significant changes designed, for the most part, to ease certain procedural requirements for the interception of such communications by federal law enforcement officers. Some of these new procedural provisions are as follows:

(a) Interception of electronic communications. 18 U.S.C. 2516(3) allows any attorney for the government to make an application for an electronic communications interception order in connection with any federal felony. This is in contrast to the enumerated crimes that limit requests for wire or oral interception orders. Moreover, the new law does not require approval from Washington as a prerequisite to filing an application for an electronic communications interception order. However, although Washington approval for this type of interception order is not required by the Act, the Department of Justice has agreed with Congress to administratively require Washington approval for the first three years to insure that the Act is properly implemented. See, H. Rep. No. 99-647, supra, at p. 51. Accordingly, for the initial three year period, requests to intercept electronic communications must be authorized by the same officials in Washington that authorize the interception of wire communications.

It is also important to note that the provisions of the legislation regulating the interception of electronic communications do not include a statutory exclusionary rule such as exists in 18 U.S.C. 2515, which prohibits the evidentiary use of illegally intercepted wire and oral communications. Instead, the Act provides that the sanctions set forth in the statute for an unauthorized interception of an electronic communication shall be the "only judicial remedies and sanctions for nonconstitutional violations" of the provisions governing electronic communications. 18 U.S.C. 2518(10)(c).

(b) Mobile interception devices. Under the prior wiretap statute, a law enforcement agency wishing to install an oral interception device in an automobile had to obtain an order authorizing the interception from a court in every district that the automobile was expected to enter or forego intercepting conversations in districts in which no order had been obtained. The new statute amends 18 U.S.C. 2518(3) by providing that court orders for mobile interception devices need only be obtained in one district. Thus, there will no longer be a need to secure separate court orders in each jurisdiction that the vehicle passes through; an order in any jurisdiction within the United States will authorize the requested interception. This provision should be available not only for oral bugging devices installed in vehicles, but for court orders authorizing interception of cellular phone conversations over car telephones. Note that in contrast with the provision on mobile tracking devices, 18 U.S.C. 3117, the authorization under 18 U.S.C. 2518(3) for mobile interception devices is valid only within the United States.

(c) Commencement of the thirty day period. 18 U.S.C. 2518(5) has been amended to provide that the thirty day period for an order authorizing the interception of a wire, oral or electronic communication begins on the earlier of the day on which the interception begins or ten days after the order is entered. This latter provision allows a grace period in case of difficulties in setting up equipment or other technical or operational problems. Thus, investigative agents will have up to ten days in which to place a listening device, often a difficult job, before the thirty day time limit begins to run on the order. This provision makes it more likely that a full interception period will take place before an extension order has to be sought.

(d) After the fact minimization. 18 U.S.C. 2518(5) has also been amended to specifically authorize after the fact minimization in cases where codes or foreign languages are used by the interceptees and there is no expert reasonably available to translate the conversations during the interception period. This amendment provides statutory authorization for what is becoming a more frequent practice as interceptees use complex codes and foreign languages in an attempt to ensure the secrecy of their conversations. Often, the codes and languages used are so obscure that it is impossible to find a translator until the interception period is well under way or over.

(e) The use of support personnel. One of the most frequent problems encountered by agencies conducting electronic surveillance pursuant to the original statute has been the need to use "law enforcement officers," as that term is defined in 18 U.S.C. 2510(7), to monitor intercepted conversations. This requirement necessitated that non-agent translators, state and local investigators, or any other individuals needed to aid in the monitoring, who were not federal law enforcement officers under the specific statutory definitions, be deputized as United States Marshals before conducting the interceptions. The deputation requirement often resulted in disputes over the meaning of "law enforcement officer" and delays in the authorization process. The problem has been eliminated by the new law, which provides that an interception may be conducted by "Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception." 18 U.S.C. 2518(5). This change is designed to substantially reduce the deputation procedure as well as free field agents from the need to monitor interceptions so that they can engage in other law enforcement activities. The key to the provision is that the government or contract personnel must be working under the supervision of an appropriate investigative or law enforcement official.

(f) Roving interceptions. One of the most significant additions to 18 U.S.C. 2518 concerns the specificity required in the description of the place to be bugged or the telephone to be tapped. The original law required that the application for, and the order authorizing, an electronic surveillance request indicate the "particular" facility or place in which the interception was to occur. The new law contains an exception to

the particularity requirement and, in effect, allows an interception order to target a specific person rather than the specific telephone or premises that that person might use. The amendments establish two similar rules to govern the interception of "oral communications" and "wire or electronic communications" where the target facility need not be identified with specificity before the interception order is obtained. 18 U.S.C. 2518(11).

With respect to "oral communications," the application must contain a full and complete statement as to why the ordinary specification requirements are not practical. The application must also identify the person committing the offense and whose communications are to be intercepted. The judge must then make a specific finding that the ordinary specification rules are not practical under the circumstances. 18 U.S.C. 2518(11)(a). Examples of situations where ordinary specification rules would not be practical include cases in which suspects meet in parking lots or fields or move from hotel room to hotel room in an attempt to avoid electronic surveillance. In such cases, the order would allow law enforcement officers to follow the targeted individual and engage in the interception once the conversation occurs. 18 U.S.C. 2518(12).

The provision concerning "wire or electronic communications" is similar to that governing oral communications. The application must specifically identify the person committing the offense whose communications are to be intercepted. The application must also show, however, that the person committing the offense has demonstrated a purpose to thwart interception by changing facilities. In these cases, the court must specifically find that such a purpose has been evidenced by the suspect. An example of a situation that would meet this test would be the subject who moves from phone booth to phone booth numerous times to avoid interception. 18 U.S.C. Section 2518(11)(b).

With respect to both oral and wire or electronic communications, the approval of the Attorney General, Deputy Attorney General, Associate Attorney General, Assistant Attorney General or an Acting Assistant Attorney General is required before a relaxed specificity order is sought. Approval by a Deputy Assistant Attorney General in the Criminal Division, which is authorized for all other interceptions, is not sufficient for this type of application.

The government cannot begin the interception until the facilities from which, or the place where, the communication is to be intercepted is determined by the agency implementing the order. 18 U.S.C. 2518(12). Congress also intended that the actual interception not commence until the targeted individual begins, or evidences an intention to begin, a conversation. It was not intended that the relaxed specificity order be used to tap a series of telephones, intercept all conversations over those phones, and then minimize the conversations recorded as a result. This provision puts the burden on the investigatory agency to determine when and where the interception is to commence. See, H. Rep. No. 99-647, supra, at p. 53. There is no requirement of notification to the court once the premises or specific phone is identified prior to making the interception; however a specific place or phone must be identified. Limiting interceptions to specific places once they are determined should satisfy the specificity requirement of the Fourth Amendment.

Obviously, this provision will be a valuable tool in criminal investigations as sophisticated suspects have been quite effective in avoiding electronic surveillance by frequently changing their meeting places and telephones. However, the Fourth Amendment implications involved in this procedure should not be ignored. This is an extraordinary provision and it is the intention of the Department of Justice that it be used sparingly and only in clearly appropriate cases. This provision is not a substitute for investigative footwork; it is not intended that the ordinary showing of probable cause with respect to a specific telephone or location be dispensed with on the theory that the subject is a criminal who engages in criminal conversations wherever he goes.

A further consideration, especially in wire or electronic interceptions, is the practical problems faced by the telephone company or other provider of electronic communication services in effecting the interception, complete with leased lines to the government listening post, on extremely short notice. Care has to be exercised to work with the telecommunication companies and to provide them with as much information and notice as possible as far in advance as possible. Telephone companies in particular have expressed great concern about their ability to comply with such orders, which may require action on their part that will strain their ability to assist law enforcement officials in these cases. Congress, at the request of the telephone companies, included a provision in the Act allowing the companies to move the court that has issued a reduced specificity order for the interception of wire or electronic communications to modify or quash the order if the interception cannot be performed in a timely or reasonable manner. 18 U.S.C. 2518(12). The key for all concerned is to approach this procedure with care and foresight and to be aware of the practical and legal problems that may arise.

(g) Reporting requirements. 18 U.S.C. 2519, which requires judicial reports to the Administrative Office of the United States Courts, has been amended to require reports on wire, oral, or electronic communication surveillance orders issued under the relaxed specificity provisions noted above. 18 U.S.C. 2519(1)(b). Otherwise the reporting section is unchanged.

9) Recovery of Civil Damages

18 U.S.C. 2520 relating to civil damages has been largely rewritten. The new section provides for equitable relief, compensatory and punitive damages, and attorneys' fees for a violation of the chapter. Added to section 2520 are statutory provisions for the computation of damages and a two year statute of limitations on actions brought under the section. Finally, 18 U.S.C. 2520(d) provides a good faith defense to actions brought under the section and specifically includes reliance on a facially valid court order within the meaning of "good faith."

(10) Injunctive Remedy

A new section, 18 U.S.C. 2521, has been added to the law. This section enables the Attorney General to initiate civil proceedings to enjoin a felony violation of the chapter that presents a continuing and substantial injury to the United States or to any person or class for whose protection the action is brought.

TITLE II - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Title II of the Act is completely new and is designed to protect the privacy of stored electronic communications, either before such a communication is transmitted to the recipient or, if a copy of the message is kept, after it is delivered. In developing legislation to cover new communications technologies, now identified by the statute as "electronic communications," it became apparent that entirely different problems exist with reference to such methods as electronic mail and computer transmissions than are present in the case of wire or oral communications. In the former, copies, whether backup to guard against computer failure or stored copies in a remote computing system, are a central feature of the new technology; in the latter, preserved copies of spoken telephone messages are virtually unknown. Businesses and companies that provide communications services urged Congress to establish appropriate methods for government access to these new stored records to protect their customers' interests and to bring certainty to this developing communications industry. In addition, privacy interests were recognized by making it a federal offense to improperly access or disclose the contents of stored electronic communications. In developing the legislation these new electronic communications were divided into two categories: a) communications during the transmission stage, and b) communications in "storage." Electronic storage is defined in 18 U.S.C. 2510(17) as both any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof and the storage of such communication by an electronic communication service for purposes of backup protection of such communication.

There was general recognition that the interception of communications during the transmission stage is more intrusive than of those in storage and, accordingly, those communications were given almost the same protection as that provided for wire and oral communications. However, as noted earlier in this memorandum, it is somewhat easier to obtain an interception order for an electronic communication in transmission than it is to obtain a wire or oral interception order. The provisions governing electronic communications during the transmission stage are set forth in Title I of the Act and are discussed in detail at p. 9, supra.

With respect to stored communications, the Department originally urged that these communications should be treated as third party records and should be available by administrative or grand jury subpoena or by a court order. The various concerned segments of the communications industry had considerable difficulty with this concept, arguing that in the business community clients would not use electronic communications services if the records being transmitted were readily available to law enforcement agencies. These communications were likened to regular mail being handled by the Post Office. Under present day standards, a search warrant would be required to intercept mail since it enjoys Fourth Amendment protection. Congress ultimately decided that electronic mail in storage incident to transmission should be accorded the same protection. 18 U.S.C. 2703(a).

The same principle applies to "backup" copies made by the providers of electronic communications services to protect the communications from loss when the system has a malfunction and records are inadvertently lost, a not infrequent occurrence. As these copies are kept to protect the owner, the argument was made that since their existence is for the owner's benefit, a search warrant should be required to obtain them just as it would be needed to seek the records if possessed at the owner's headquarters. Similar protection was requested for records maintained by providers of remote computing services that were simply performing processing functions and did not have access to the contents of the communications. Without the right to actually access the records, the claim was made that the remote computing service provider was not truly a third party custodian. An example of a remote computing service would be a firm that takes time and salary records from a large firm, applies established computer programs to the records, and returns pay checks with appropriate tax deductions made.

The consensus that was reached was to accord Fourth Amendment type protection to the stored data for the first 180

days, requiring a search warrant under Rule 41 of the Federal Rules of Criminal Procedure for government access. After the 180-day period expired, any records still retained would revert to the status of third party records and would be available by administrative or grand jury subpoena or by a specially created court order procedure. The Act's provisions also permit the government to ask a computer storage company to create a copy of existing records as they exist on a specific day and hold them pending court order access. This provision, to be discussed infra, should be quite beneficial in certain large scale fraud investigations where remote computing facilities are used as it will eliminate the danger of a computer command to destroy the records when the perpetrator suspects law enforcement interest in his activities.

The most important provisions of Title II are the following:

(1) Unlawful Access to Stored Communications

18 U.S.C. 2701 makes it an offense to (a) intentionally access, without authorization, a facility through which an electronic communication service is provided; or (b) intentionally exceed the authorization of such facility; and as a result of this conduct, obtain, alter or prevent authorized access to a wire or electronic communication while it is in electronic storage in such a system. 18 U.S.C. 2701(a). An "electronic mail" service, which permits a sender to transmit a digital message to the service's facility, where it is held in storage until the addressee requests it, would be subject to 18 U.S.C. 2701. A "voice mail" service operates in much the same way, except that the stored message takes the form of the sender's voice, usually in digital code. It would likewise be subject to this section. Moreover, a remote computing service provided through an electronic communication service is also protected.

This provision is intended to address the increasing problem of both unauthorized "computer hackers" and corporate spies who deliberately gain access to, and sometimes tamper with, electronic communications that are not available to the public. The provision is not intended to criminalize access to "electronic bulletin boards," which are generally open to the public so that interested persons may communicate on specific topics. Where communications are readily accessible to the general public, the sender has, for purposes of 18 U.S.C. 2701(a), extended an "authorization" to the public to access those communications. A communication will be found to be readily accessible to the general public if the telephone number of the system and other means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy. To access a communication on such a system is not a violation of the law. 18 U.S.C. 2701(a).

If a violation of 18 U.S.C. 2701(a) was committed for commercial advantage, malicious destruction or damage, or private financial gain, the violator could receive up to a year in prison and a $250,000 fine for the first offense and up to two years imprisonment and a fine as provided by Title 18, United States Code, for a second or subsequent offense. In all other cases, a jail term of up to six months and a fine of $5,000, or both, could be imposed. 18 U.S.C. 2701(b)(2).

(2) Disclosure of the Contents of a Stored Communication

18 U.S.C. 2702 governs disclosure of the contents of a stored communication. 18 U.S.C. 2702(a) generally prohibits the provider of a wire or electronic communication service from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient of the communication. Similarly, 18 U.S.C. 2511(3), as amended, prohibits such a provider from divulging the contents of a communication while it is in the transmission stage. Neither provision, however, nor any other provision of the Act, is intended to affect any other provision of federal law that prohibits the disclosure of information on the basis of the content of the information, such as the Fair Credit Reporting Act, 15 U.S.C. 1681(b), which limits the circumstances under which consumer reporting agencies may disclose certain information relating to consumers.

-A-77-

18 U.S.C. 2702(a)(1) states that a provider of an electronic communication service shall not knowingly divulge the contents of a communication while in electronic storage.

18 U.S.C. 2702(a)(2) prohibits the provider of a remote computing service from disclosing the contents of any communication that is maintained by the service if certain conditions are met. The first condition is that the communication must be on behalf of and received by means of electronic transmission from (or created by means of computer processing of communications received by means of transmission from) a subscriber or customer of such service. 18 U.S.C. 2702(a)(2)(A). The second condition is that the communication must be solely for the purpose of providing storage or computer processing services to the subscriber or customer if the provider is not authorized to access the contents of any such communications for purposes of providing services other than storage or computer processing. 18 U.S.C. 2702(a)(2)(B). The practical purpose of this provision was set forth in the Report of the House of Representatives Committee on the Judiciary as follows:

> This provision reflects the rapidly growing importance of information storage and processing to the Nation's commerce. Today, the subject matter of commerce increasingly is information in electronic form and the processing of information itself has become a major industry. The secure storage of electronic information has thus become as important to the commercial system as the protection of paper records. Accordingly, where an electronic communication is transmitted by a subscriber or customer to such a service, and is stored on the subscriber's behalf solely for the purpose of providing storage or computer processing services to the subscriber, the Committee intends that the communication - - together with the products of any processing that the service performs for the customer - - remain available only to the subscriber and to the persons he designates, with certain exceptions enumerated in Section 2702(b). H. Rep. No. 99-647, <u>supra</u>, pp. 65-66.

18 U.S.C. 2702(b) provides six distinct exceptions that modify the general prohibitions against disclosure contained in 2702(a). Accordingly, the contents of a communication may be disclosed under the following circumstances:

a. to an addressee or intended recipient of the communication or his agent;

b. as otherwise authorized in 18 U.S.C. 2517 (the basic wire and electronic communications disclosure provisions); 18 U.S.C. 2511(2)(a) (disclosure to suitable switchboard operators and telephone company personnel in the ordinary course of business); or the new 18 U.S.C. 2703 (access by the government to the contents of electronic communications);

c. with the consent of the originator, addressee, or intended recipient, or the subscriber in the case of a remote computing service;

d. to an employee or other person whose facilities are used to transmit the communication to its destination;

e. as may be necessary in order to provide the service or to protect the property or rights of the provider of the service;

f. to a law enforcement agency, if the contents were:

(i) inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime.

The final exception is intended to be read narrowly. It is not intended to be a substitute for fulfilling the procedural requirements contained in 18 U.S.C. 2703, which govern government access to stored communications. A service provider's systematic practice of reviewing these communications to look for evidence of a crime would not qualify as inadvertent. H. Rep. No. 99-647, *supra*, at p. 67.

It should be noted that the penalty for improper disclosure by a service provider of stored communications is civil in nature since this section provides no criminal penalty. A provision for a civil action for violation of most of the provisions of Title II of the bill is set out in the new 18 U.S.C. 2707.

(3) Requirements for Governmental Access to Stored Communications

(a) Procedures for access to the contents of a stored communication. 18 U.S.C. 2703 sets forth the procedural requirements that the government must meet in order to obtain access to electronic communications in storage and related transactional records. The statute draws a distinction between contents of electronic communications that have been in storage for 180 days or less and those that have been stored for a longer period of time. Thus, the section provides that a governmental entity may only obtain access to the contents of an electronic communication that has been in storage for 180 days or less pursuant to a search warrant issued under the Federal Rules of Criminal Procedure or an equivalent state warrant. If the message has been stored for more than 180 days the government can, as discussed below, obtain the information by a variety of procedures including a search warrant, grand jury subpoena, administrative subpoena, or a court order, depending on the type of notification the government wishes to provide the subscriber. The distinction results from Congress's conclusion that while the contents of a message in storage should be protected by Fourth Amendment standards as are the contents of a regularly mailed letter, to the extent that the record is kept beyond six months, it is closer to a business record maintained by a third party for its own

benefit and, therefore, deserving of a lessened standard of protection. The above provision clearly applies to the new communication concept generally referred to as electronic mail in which messages are sent between parties much like traditional mail except that an electronic communications system is utilized instead of a postal service. As noted below, the provision, with its search warrant requirement, may not apply in the case of a remote computing service in which a data base may be held by the service for less than or more than 180 days and can be modified and updated on a weekly or even a daily basis.

18 U.S.C. 2703(b) sets forth the procedures that the government may use to obtain access to electronic communications held for more than 180 days or to such communications held by a provider of a remote computing service. That subsection provides that the government may proceed using any of three alternative means of access. The government may, without providing any notice to the subscriber, obtain a state or federal search warrant based upon probable cause. 18 U.S.C. 2703(b)(A). If the government chooses to give notice to the subscriber, it may obtain access to the records by using either a grand jury or administrative subpoena, 18 U.S.C. 2703(b)(B)(i), or a new statutory court order based upon a finding that the records are relevant to a legitimate law enforcement inquiry. 18 U.S.C. 2703(d). Please note that the required notification to the subscriber may be delayed pursuant to 18 U.S.C. 2705, as discussed below.

As noted, 18 U.S.C. 2703(a), which governs the procedures for governmental access to the contents of records in electronic storage, requires that a search warrant based on probable cause be obtained for access to the contents of an electronic communication held for less than 180 days. Such communication contents held for more than 180 days can be obtained by the methods set forth in 18 U.S.C. 2703(b), which, along with search warrants, include a specially created court order and grand jury and administrative subpoenas. 18 U.S.C. 2703(b) relates specifically to records held in remote computing systems and such records are not mentioned anywhere in 18 U.S.C. 2703(a). The question arises as to whether the 180 day provision in 18 U.S.C. 2703(a) applies as well to records held in remote computing systems as it clearly does to communications during transmission such as those utilized by an electronic mail company. Is access to records held by remote computing systems limited during the first 180 days in the system to situations where search warrants can be obtained, or can those records be accessed by the government, regardless of their length of time in the system, simply by use of a grand jury or administrative subpoena or the new statutory court order?

The Act is clearly disjunctive in its treatment of "Electronic Communications in Electronic Storage" under 18 U.S.C. 2703(a) and "Electronic Communications in a Remote Computing Service" under 18 U.S.C. 2703(b). It would appear, therefore, that Congress intended that access to communications in a remote computing service be governed only by the provisions of 2703(b), which makes a search warrant optional to a subpoena or court order. Since no time limit is set forth in 2703(b), it seems that the government could obtain records in a remote computing service at any time by issuing an administrative or grand jury subpoena or obtaining a court order based upon a simple showing of relevancy. The legislative histories of the Act, however, make this proposition far from clear.

The House Report treats communications in electronic storage and communications in a remote computing system in the disjunctive, as the Act itself does. Thus, the House Report states that 18 U.S.C. 2703(a) deals with the contents of an electronic communication in storage, noting that such records can only be obtained through a search warrant during the first 180 days in storage. H. Rep. No. 99-647, _supra_, at pp. 67-68. The House Report also notes that "electronically stored communications can be of two types. The first type of stored communications are those associated with transmission and incident thereto. The second type of storage is of a back-up variety." _Id_. at p. 68. This statement, and the fact that remote computing service records are discussed under a separate subsection in the House Report, supports the view that records given to a remote computing service are neither given over for, nor held incidentally to, purposes of transmission and, therefore, are not governed by the 180 day provisions set forth in 18 U.S.C. 2703(a).

The Senate Report, however, appears to treat the two types of records in the same manner in stating that 18 U.S.C. 2703(b) "provides that for electronic communications that are maintained by a remote computing service _and_ that have been in storage in an electronic communication service for more than 180 days the Government can gain access in several ways." S. Rep. No. 99-541, 99th Cong., 2d Sess. at p. 38 (1986). The Senate Report contains no independent discussion of remote computing service records in storage for less than 180 days. The argument can be made that the Senate Report is incorrect as it does not reflect the plain meaning of the statute as set forth in 18 U.S.C. 2703(a) and (b). Moreover, since the language was originally drafted by the House, the House Report should be the more authoritative as the Senate made no changes in this language.

Although it does not appear in either Report, an argument can be made that because a remote computing company has little access to the records themselves, they are

-A-79-

nothing more than a mere extension of the record originator and should stand in the originator's place in the face of a government request for access to the records. If a search warrant would be required to obtain the originator's records in his own office, then, similarly, a search warrant should be necessary to obtain the same records from a remote computing service possessing the records under circumstances in which the service cannot access the records except for purposes of storage or to run a computer program. Without independent access to the records, the remote computing service should not be deemed an ordinary third party custodian of records who must respond to a subpoena. This is the argument the remote computing industry is sure to raise.

Ultimately, the courts will have to determine the correct legislative meaning and intent on this issue. Initially, United States attorneys are urged to argue that government access to the contents of an electronic communication held by a remote computing service does not require a search warrant during the first 180 days. All those implementing this statute for the government should be aware, however, that this ambiguity exists and be prepared for a court challenge to a subpoena or the more limited statutory court order for such records.

As just referred to above, the type of electronic communication held by a remote computing service that is subject to these provisions on governmental access is limited. The communication must be on behalf of a subscriber of a remote computing service and must have been given to the remote computing service under narrow conditions. The communication must have been received in a certain form (_i.e._, by means of electronic transmission or similar means). 18 U.S.C. 2703(b)(2)(A). In addition, the communication must have been surrendered solely for the purpose of providing storage or computer processing services to the subscriber, and the provider may not be authorized to access the contents of any such communication for purposes of providing any services other than storage or computer processing. 18 U.S.C. 2703(b)(2)(B). A computer storage company that does not meet these requirements would certainly be deemed an ordinary third party custodian of records regardless of the ultimate decision as to the remote computing service.

(b) Procedures for access to transactional information including telephone toll records. 18 U.S.C. 2703(c) sets forth the rules under which the government may obtain access to transactional records. These are records that pertain to the subscriber to, or customer of, an electronic communication service or remote computing service and which do not involve the contents of a communication. In electronic communications these are the records that are the equivalent of the traditional telephone toll records maintained by a telephone company. As drafted, this provision covers not only transactional records of an electronic mail company or a computer data processor, but also, in fact, covers and regulates governmental access to traditional telephone toll records themselves. It is important to note at the outset that the statute's provisions in the area of telephone toll records impose no greater burden on the government than the previous Department policy of obtaining such records by way of subpoena or administrative summons. In fact, in some cases, the statute will actually make it easier for an investigative agency to obtain and use such records. Nevertheless, as part of the general intent of the Act to cover all forms of wire and electronic communications, telephone toll records, like pen registers, will now be covered by a federal statute.

As discussed below, the government will be able to obtain such transactional records by grand jury subpoena, administrative subpoena, or court order based upon a finding of relevancy. In the past, the Federal Bureau of Investigation could only obtain these records pursuant to a grand jury subpoena with such a subpoena's attendant Rule 6(e) disclosure and storage restrictions and problems. Under 18 U.S.C. 2703(c), the Bureau, and other investigative agencies lacking administrative subpoena powers, will now be able to obtain transactional records, including telephone toll records, pursuant to a court order based on a readily available standard and telephone toll records available solely as grand jury records will no longer be a problem.

18 U.S.C. 2703(c)(1)(B) and 18 U.S.C. 2703(c)(2) allow the government to obtain transactional records without notice to the subscriber by obtaining (1) an administrative or grand jury subpoena; (2) a search warrant pursuant to state or federal law; or (3) a court order pursuant to 18 U.S.C. 2703(d) based upon a finding that the information is relevant to a legitimate law enforcement inquiry. Granted that pen register data (regulated in Title III of the Act) and telephone toll records provide identical type data, that court process of some nature is now required under Department policy for such records, and that the Act's intent is to regulate all forms of wire and electronic communications, this provision with its relevancy standard both effectuates the Congressional purpose and protects legitimate law enforcement interests in obtaining the necessary information. The government may also, of course, obtain such records from the service provider when the customer consents to the disclosure. 18 U.S.C. 2703(c)(1)(B)(iv).

(c) Court orders for disclosure of the contents of communications or transactional records. 18 U.S.C. 2703(d) governs court orders issued pursuant to 18 U.S.C. 2703(b)(B)(ii) relating to the contents of stored communications and 18 U.S.C. 2703(c)(1)(B)(iii) relating to transactional records. 18 U.S.C. 2703(d) provides that to obtain such an order the government must demonstrate that there is reason to believe that the contents of an electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. The only contents that can be sought using the court order option are those stored for more than 180 days. Thus, the standard for the order for contents of records stored more than 180 days is the same as for transactional records. However, for contents, as opposed to transactional records, notice to the subscriber is also required unless it can be delayed under 18 U.S.C. 2705; no notice is required to the subscriber for access to transactional records.

(d) Cause of action barred. 18 U.S.C. 2703(e) provides that no cause of action shall lie against the provider of a wire or electronic communications service, or its officers and employees, for providing information, facilities, or assistance to the government pursuant to a court order, subpoena, warrant or certification.

(4) Backup Preservation of Information in Storage

(a) Government access. 18 U.S.C. 2704 sets forth the procedures that apply to backup copy preservation. This is the provision that will permit law enforcement officials to have a copy, in the nature of a picture of the records that exist on a given day, made of records of illegal activities in which a computer storage or remote processing firm is utilized in the criminal activity. It is an innovation that should be of major value to law enforcement in coming years. 18 U.S.C. 2704(a)(1) provides that when the government seeks records that are being held by a remote computing storage company pursuant to 18 U.S.C. 2703(b)(2), the government may include in its subpoena or court order a requirement that the service provider create a backup copy of the communication in order to preserve the communication. The provider is directed to create the requested backup copy as soon as practicable consistent with its regular business practices, but in any event within two business days of the receipt of the order or subpoena and then notify the government that the copy has been made. The provider is also directed not to notify the subscriber of the order or subpoena.

18 U.S.C. 2704(a)(2) provides that the government is required to notify the subscriber of the subpoena or court

order within three days after the receipt of the service provider's confirmation of the creation of the backup copy. This notice can be delayed pursuant to 18 U.S.C. 2705(a). 18 U.S.C. 2704(a)(3) states that the provider may not destroy the backup copy until the later of (1) the delivery of the information to the government; or (2) the resolution of any legal proceedings related to the government's order or subpoena.

Under 18 U.S.C. 2704(a)(4) the service provider is required to release the backup copy to the government no sooner than 14 days after the government provides notice to the subscriber if (1) the provider has not received notice that the subscriber has challenged the government's request; and (2) the provider has not initiated proceedings to challenge the subpoena or court order.

18 U.S.C. 2704(a)(5) provides that a government agency may require the creation of a backup copy under 2701(a)(1) if in <u>its sole discretion</u> the agency determines that there is reason to believe that notification pursuant to 18 U.S.C. 2703 of the existence of a subpoena or court order for the production of stored communications may result in the destruction of or tampering with the evidence sought. It is of special significance that this determination is not subject to challenge by the subscriber or service provider. The key to this provision is that the government can make certain that a copy of the relevant records is created prior to any litigation or notice and before any attempt to alter or destroy the records electronically can be made.

(b) Customer challenges. 18 U.S.C. 2704(b)(1) provides that within 14 days after notice by the government that a backup copy has been requested, the subscriber may move to vacate the court order or quash the subpoena ordering that the backup copy be made. The subsection then sets forth the procedural details governing proceedings to quash or vacate. The challenger must serve the government with notice and provide written notice to the service provider. The challenger must then establish that he is the relevant customer or subscriber and that the records sought are not relevant to a legitimate law enforcement inquiry or that the government failed to comply with the statutory requirements for access to the records.

If the court finds that the challenger has met the requirements of 2704(b)(1), the government must file a sworn response, <u>in camera</u> if appropriate. 18 U.S.C. 2704(b)(3). If the court determines that the challenger has failed to meet these requirements, it will order the process enforced. On the other hand, if the challenger has standing and can show either lack of relevance or noncompliance with the procedural requirements, the court can vacate the order or

quash the subpoena. 18 U.S.C. 2704(b)(4). Thus, once the backup copy is created, the government can enforce access to it by complying with the procedural provisions of this section and by merely establishing relevancy to a legitimate law enforcement inquiry.

18 U.S.C. 2704(b)(5) provides that a court order denying a motion or application shall not be deemed a final order and, therefore, no interlocutory appeal may be taken from the denial. Of course, nothing precludes a subscriber from raising these issues again during a subsequent hearing or trial.

(5) <u>Delayed Notice</u>

(a) Procedure. 18 U.S.C. 2705 governs delay of notification to the customer or subscriber. Where the government seeks the contents of a stored electronic communication pursuant to the provisions of 18 U.S.C. 2703(b) by way of a court order, it may include in its application a request for delayed notification of 90 days or less. The court is to grant this request if it determines that there is reason to believe that notification might have an adverse result as described in 2705(a)(2). 18 U.S.C. 2705(a)(1)(A). Where the government seeks the contents of a communication governed by 18 U.S.C. 2703(b) by way of an administrative or grand jury subpoena, it may obtain a delay of notification for a period of up to 90 days upon the certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in 2705(a)(2). 18 U.S.C. 2705(a)(1)(B). It should be noted that under this latter provision, the government need provide only the written certification; it is not necessary for the government to obtain a court order based upon a finding of adverse results. Thus, this provision, unlike similar delayed notification provisions in statutes such as the Right to Financial Privacy Act, 12 U.S.C. 3409, requires nothing more than a government certification to trigger delayed notification.

A "supervisory official" for purposes of this provision includes the investigative agent or assistant investigative agent in charge of a field office or an equivalent official in the investigating agency's headquarters or regional office. Thus, for instance, it will require the certification of a supervisory agent such as the Special Agent in Charge or the Assistant Special Agent in charge of an FBI or DEA office to comply with this provision. A certification by the agent in charge of an investigation would not suffice. The term also means the chief prosecuting attorney, the first assistant or an equivalent official in a regional or headquarters office. 18 U.S.C. 2705(a)(6).

18 U.S.C. 2705(a)(4) provides that extensions of up to 90 days may be made of the delayed notification as long as the original requirements of the section are met with respect to the extension.

(b) Adverse results. An adverse result that can trigger delayed notification is one of the following: (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of, or tampering with, evidence; (4) intimidation of potential witnesses (including victims of any crimes); and (5) otherwise seriously jeopardizing an investigation or unduly delaying an ongoing trial. 18 U.S.C. 2705(a)(2).

(c) Preclusion of notification. 18 U.S.C. 2705(b) provides a procedure for the government to preclude the service provider from notifying its customer or subscriber of the existence of a warrant, subpoena, or court order. That section states that such preclusion may only be obtained in cases where the government is not required to notify, or where the government has obtained the authority to delay notification. A preclusion of notification must be granted by a court of competent jurisdiction that finds that there is reason to believe that adverse results set forth in 18 U.S.C. 2705(a)(2) will occur if notification is given.

(6) Cost Reimbursement

(a) Payment. 18 U.S.C. 2706(a) provides that the government, when seeking records pursuant to 18 U.S.C. 2702, 2703, or 2704, must reimburse the person or entity assembling or providing the records for all reasonable costs that have been incurred in providing the information. Note that 18 U.S.C. 2706(c) exempts telephone toll records and telephone listings from the reimbursement requirement. These records are excluded primarily because the government has not traditionally paid the telephone companies for providing this type of information. The court can, however, order the government to reimburse the provider of telephone toll records where the information sought is unusually voluminous or causes an undue burden on the provider. 18 U.S.C. 2706(c).

(b) Amount. Under 18 U.S.C. 2706(b), the amount of the reimbursement payment will be as mutually agreed by the government and the provider or, in the absence of such an agreement, as determined by the court.

(7) Civil Action

(a) Cause of action. 18 U.S.C. 2707(a) provides a civil cause of action for a provider of an electronic communication service, or its customer or subscriber who is aggrieved by an intentional violation of the statute. However, this provision and 18 U.S.C. 2703(e) specifically preclude any cause of action against a provider of an electronic communication service that discloses information pursuant to a court order, warrant, subpoena or certification.

(b) Relief. 18 U.S.C. 2707(b) defines the relief that may be appropriate in civil actions to include preliminary or other equitable or declaratory relief, damages, attorneys' fees, and other reasonably incurred litigation costs. Damages include actual damages and any profits made by the violator as a result of the violation, but in no case less than $1,000. 18 U.S.C. 2707(c).

(c) Defenses. 18 U.S.C. 2707(d) sets forth the defenses to actions brought under the statute. This subsection provides a complete defense to any civil or criminal action brought under Title 18, United States Code, or any other law where the defendant demonstrates a good faith reliance on a court order, warrant, subpoena, or legislative or statutory authorization, or in good faith complies with a request from a law enforcement officer. 18 U.S.C. 2707(d) also provides a complete defense to defendants who rely upon a good faith determination that 18 U.S.C. 2511(3) permitted the conduct complained of.

(d) Statute of limitations. 18 U.S.C. 2707(e) provides that a civil action may not be commenced later than two years after the date upon which the claimant first discovered or had reasonable opportunity to discover the violation.

(8) Exclusivity of Remedies

18 U.S.C. 2708 provides that the remedies and sanctions described in the statute are the only judicial remedies and sanctions available for nonconstitutional violations of the Act. When a violation of constitutional magnitude is involved, the trial court will apply the existing constitutional law with respect to the exclusionary rule. United States v. Leon, 468 U.S. 897 (1984).

(9) Counterintelligence Access to Telephone Toll and Transactional Records

(a) Duty to provide. 18 U.S.C. 2709 sets forth the rules governing counterintelligence access to telephone toll and transactional records. 18 U.S.C. 2709(a) provides that a communications common carrier or the provider of an electronic communication service shall provide such subscriber information or telephone toll records pursuant to a request from the Director of the Federal Bureau of Investigation under 18 U.S.C. 2709(b).

(b) Certification. 18 U.S.C. 2709(b) contains the conditions under which the Director of the FBI, or his designee, may request these records. This section states that the Director or his designee must certify in writing that the information sought is relevant to an authorized foreign counterintelligence investigation; and that there are specific, articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1801 et seq.

(c) Disclosure prohibition. 18 U.S.C. 2709(c) prohibits the service provider from disclosing to any person that the FBI has sought or obtained transactional records under the provisions of 18 U.S.C. 2709.

(d) Dissemination by the FBI. 18 U.S.C. 2709(d) provides that the FBI may disseminate records obtained under this section only as provided in guidelines approved by the Attorney General for foreign counterintelligence collection and foreign counterintelligence investigations conducted by the FBI, and with respect to dissemination to an agency of the United States the dissemination can only be made if the information is clearly relevant to the authorized responsibilities of such agency.

(e) Congressional consultation. 18 U.S.C. 2709(e) provides that the Director of the FBI shall fully inform the House and Senate intelligence committees concerning all requests made under this section.

TITLE III - PEN REGISTER AND TRAP AND TRACE DEVICES

The final Title of the legislation adds a new Chapter 206 to Title 18 of the United States Code, Section 3121 et seq., which regulates the use of pen registers and trap and trace devices. The title begins with a general prohibition against the use of a pen register or a trap and trace device without first obtaining a court order pursuant to 18 U.S.C. 3123 or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.). Although the courts have clearly held that pen registers were not within the reach of the wiretap statute and that the Fourth Amendment does not

require a warrant for this procedure, (United States v. New York Telephone Co., 434 U.S. 159 (1977); Smith v. Maryland, 442 U.S. 735 (1979)), the telephone companies have insisted on court orders for fear of civil liability before they would assist in placing a pen register. The same principle has applied to trap and trace devices. Accordingly, for a number of years Department policy has required the use of a court order issued under Rules 41 or 57 of the Federal Rules of Criminal Procedure for pen registers and trap and trace devices. USAM 9-7.014; 7.231. Thus, this new chapter in Title 18 in essence codifies the existing Department policy of obtaining a court order to authorize the installation of a pen register or a trap and trace device and sets forth the procedure for seeking such an order. It is important to note that the chapter places no new restrictions on law enforcement in this regard in that it applies basically the same standards required now. In addition, it has certain procedural changes that are advantageous to law enforcement. Moreover, codifying the pen register and trap and trace procedures should eliminate the risk of more restrictive legislation, such as that contained in the original bills in this area, from being enacted in the future.

The statute contains provisions excepting the use of pen registers and trap and trace devices from the court order requirement in certain circumstances. Thus, a service provider need not obtain a court order before using a pen register or trap and trace device in order to test, operate, or maintain its equipment and services, or to protect the property rights of its customers. 18 U.S.C. 3121(b)(1). The service provider may also use a pen register or trap and trace device without first securing a court order to record the fact that a wire or electronic communication was initiated or completed in order to protect itself, or another provider, or a customer from fraud or abuse. 18 U.S.C. 3121(b)(2). Finally, it is not necessary to obtain a court order when the telephone user consents to the installation of the pen register or trap and trace device. 18 U.S.C. 3121(b)(2).

(1) Procedure

(a) The application. 18 U.S.C. 3122(a)(1) provides that any attorney for the government may apply for a pen register or trap and trace order or an extension of such an order under 18 U.S.C. 3123. The application must be in writing and under oath. It must identify the agency conducting the investigation and the person making the application and must contain a certification that the information likely to be obtained is relevant to an ongoing criminal investigation.

Please note that the standard for obtaining the order is relevancy to an ongoing criminal investigation, not probable cause or reasonable suspicion. This lesser standard reflects that while Congress wished to provide some protection against the random use of these devices, it recognized that an individual does not have a reasonable expectation of privacy in the numbers dialed to or from his telephone and, therefore, that the installation and use of a pen register or trap and trace device is not a "search" within the meaning of the Fourth Amendment requiring the protection of a warrant based upon probable cause. See, Smith v. Maryland, 442 U.S. at 743-44.

18 U.S.C. 3122(a)(2) provides that a state investigative or law enforcement officer may apply for a pen register or trap and trace order "[u]nless prohibited by State law." This phrase was included in the section to make it clear that the new law does not preempt any existing state laws governing the installation and use of pen registers and trap and trace devices by state officials. Thus, a state law requiring a higher standard of proof as a prerequisite to a pen register or trap and trace order will continue in effect with respect to that state's officials.

(b) The order. 18 U.S.C. 3122 provides that a pen register or trap and trace order may be issued by "a court of competent jurisdiction." The definition of court of competent jurisdiction includes any "district court of the United States (including a magistrate of such a court)." 18 U.S.C. 3126(2)(A). This definition, and, indeed this title, finally provides the magistrates with unquestioned authority to issue pen register and trap and trace orders. The problem prior to this provision was that although magistrates have authority under Rule 41 of the Federal Rules of Criminal Procedure to authorize the use of pen registers, there are no statutes, rules, or reported case law indicating whether magistrates could issue the ancillary technical assistance orders, and the telephone companies have refused to honor such an order issued by a magistrate. It was therefore the Department's policy that pen register and trap and trace orders be obtained only from district court judges. As noted, the definition of "court of competent jurisdiction" in section 3126 now makes it clear that a magistrate may issue enforceable pen register and trap and trace orders. See 18 U.S.C. 3124.

18 U.S.C. 3123 sets forth the procedure that must be followed by the court in issuing a pen register or trap and trace order. The section contains four subsections as follows:

Subsection (a) states that upon an application the court shall issue an ex parte order authorizing the

installation and use of a pen register or trap and trace device within the jurisdiction of the court if the court finds that the government attorney has certified that information likely to be obtained through the pen register or trap and trace is relevant to an ongoing criminal investigation. This provision does not authorize the court to conduct an independent judicial review of whether the application meets the relevance standard; it need only review the completeness of the attorney's certification. Accordingly, there will be no need for an affidavit to establish a factual basis; all that will be required is a sworn application containing the requisite certification and a draft order for the court to issue. This, too, comports with current practice.

Subsection (b) sets forth the contents of the pen register or trap and trace order. The order is required to specify (1) the identity, if known, of the person to whom is leased, or in whose name is listed, the telephone line to which the device is to be attached; (2) the identity, if known, of the person who is the subject of the criminal investigation; (3) the number and, if known, physical location of the telephone line to which the pen register or trap and trace is to be attached; and (4) a statement of the offense to which the information likely to be obtained by the device relates. In addition, the order is to direct, upon request, the furnishing of information, facilities and technical assistance necessary to accomplish the installation of the device from the service provider. The content of the order relating to cooperation is intended to codify the existing informal practice of cooperation between the telephone companies and the Department. The subsection on the required order contains largely the same requirements now imposed on federal prosecutors for a pen register order as set forth in the United States Attorneys' Manual. USAM 9-7.014, 9-7.925 and 9-7.926.

Subsection (c) provides that an order may authorize the use of a pen register or trap and trace device for a 60 day period, with possible extensions of 60 days. This is a doubling of the 30 day period now set out in the existing Department policy and should serve to limit the number of such repetitive orders.

Subsection (d) directs that the order be sealed until otherwise ordered by the court. This subsection also prohibits the disclosure of the existence of either the order or the underlying investigation to any unauthorized person unless or until otherwise ordered by the court. Violations of this provision will be punishable as a contempt of court.

(c) Technical assistance. 18 U.S.C. 3124 governs technical assistance orders. 18 U.S.C. 3124(a), which relates to pen register technical assistance orders, provides that upon the request of an authorized person a provider of a wire communication service, landlord, custodian, or other person shall furnish all the information, facilities, and technical assistance necessary to effectuate the order unobtrusively and with a minimum of interference. This is patterned on the same provision in 18 U.S.C. 2518 for assistance in the installation of a wiretap.

18 U.S.C. 3124(b) regulates technical assistance orders for trap and trace devices. The installation of these devices requires more in the way of telephone company assistance than does the installation of a pen register. Thus, this subsection states that the provider of a wire communication service, landlord, custodian, or other person shall install the trap and trace device on the appropriate line and provide all other necessary technical assistance. The subsection also requires that the third party furnish the results of the trap and trace device to the designated law enforcement agency at reasonable intervals during regular business hours for the duration of the order.

It should be noted that the telephone companies have requested, and the Department has agreed, that trap and trace technical assistance applications contain the following language that reflects the technical and business hour requirements unique to trap and trace orders:

i. the tracing operation is to be limited to Electronic Switching System (ESS) or No. 5 cross-bar facilities;

ii. the tracing operation is to be restricted to tracing and recording only those calls originating from a specific city within a certain mileage radius or, in the case of a large city, from a specific section or sections of that city; and

iii. the tracing operation is to be restricted to certain specific hours daily.

This specific language is currently required by Department policy, and, although not included in the statute, Department policy will be to continue this practice until changing technology requires modification. USAM 9-7.927 and 7.928.

18 U.S.C. 3124(c) states that the persons providing technical assistance shall be reasonably compensated for reasonable expenses incurred in providing technical

facilities and other assistance. This compensation provision is also modeled after the provision that applies in Chapter 119 of Title 18 concerning wiretap orders and is intended to be interpreted and implemented in a similar fashion.

18 U.S.C. 3124(d) provides that no cause of action shall lie against the provider of a wire or electronic communication service or its employees for providing technical assistance as required by a court order issued pursuant to this section.

Finally, 18 U.S.C. 3124(e) provides that a good faith reliance upon a court order or a legislative or statutory authorization is a complete defense to any civil or criminal action brought under this chapter or any other law.

(2) <u>Pen Register and Trap and Trace Reports</u>

18 U.S.C. 3125 requires the Attorney General to make an annual report to Congress on the number of pen register and trap and trace orders applied for by law enforcement agencies of the Department of Justice. Current Department policy already requires that the Department's agencies compile quarterly statistics concerning their pen register usage. (Memorandum of September 24, 1979, to investigative agencies from Philip B. Heymann, Assistant Attorney General, Criminal Division.) This section merely requires that this information be reformulated, with the added trap and trace data, and submitted to Congress. As there are relatively few trap and trace orders there should be little added burden caused by this reporting requirement.

UNITED STATES DISTRICT COURT
_________ DISTRICT OF ______

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES FOR AN ORDER)
AUTHORIZING THE INTERCEPTION OF)
ELECTRONIC COMMUNICATIONS)

APPLICATION

_________________, an attorney of the United States Department of Justice, states:

A. Applicant is an "investigative or law enforcement officer of the United States" within the meaning of Section 2510(7) of Title 18, United States Code, that is, an attorney authorized by law to prosecute or participate in the prosecution of all violations of federal law.

B. Applicant is also an "attorney for the Government" as defined in Rule 54(c) of the Federal Rules of Criminal Procedure, and, therefore, pursuant to Section 2516(3) of Title 18, United States Code is authorized to make an application to a Federal judge of competent jurisdiction for an order authorizing or approving the interception of an electronic communication.

C. This application seeks authorization to intercept electronic communications of _____________________________ and others as yet unknown, concerning felony violations of federal law, that is violations of __(charactize offenses)____________

____

______________________________, which have been committed and are being committed by ________________________ and others as yet unknown.

D. Applicant has discussed all the circumstances of the above offenses with Special Agent ___________________ of the (investigative agency)____ who has directed and participated in the conduct of the investigation herein, and has examined the affidavit of Special Agent _________________________ (attached to this application as Exhibit ___ and which in its entirety is incorporated by reference herein) which alleges the facts therein to show that:

1. There is probable cause to believe that _______________ _______________ and others as yet unknown, have committed and are committing felony offenses in violation of Section(s) _______________________ of Title _____ of the United States Code.

2. There is probable cause to believe that particular electronic communications of ____________________________ and others as yet unknown, concerning these offenses will be obtained through the interception for which authorization is herewith

continue until communications are intercepted that reveal the manner in which ____________________ and others as yet unknown participate in the specified offenses and that reveal the identities of (his) (her) (their) coconspirators, their places of operation, and the nature of the conspiracy involved therein, or for a period of (not to exceed 30) days, whichever is earlier; pursuant to Section 2518(5) of Title 18, United States Code, the time set forth in the order shall run from the earlier of the day on which the investigative or law enforcement officer first begins to conduct the interception or ten days from the date of this order.

(It is further ordered that special agents of the (investigative agency) are authorized to enter the foregoing premises surreptitiously for the purposes of installing, maintaining, and removing any electronic oral interception devices utilized pursuant to the authority granted by this order.)

PROVIDING THAT, this authorization to intercept (wire) (oral) communications shall be executed as soon as practicable after the signing of this order and shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under Chapter 119 of Title 18 of the United States Code, and must terminate upon attainment of the authorized objective or, in any event, at the end of (not to exceed 30) days measured from the earlier of the day on which the investigative or law enforcement officer first begins to conduct the interception or ten days from the date of this order.

PROVIDING ALSO, that (<u>applicant</u>) shall provide the court with a report on or about (<u>such intervals as the court may require</u>) days following the date of this order showing what progress has been made toward achievement of the authorized objective and the need for continued interception.

JUDGE

Date

UNITED STATES DISTRICT COURT
________ DISTRICT OF ________

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES FOR AN ORDER)
AUTHORIZING THE INTERCEPTION OF)
ELECTRONIC COMMUNICATIONS)

ORDER

AUTHORIZING INTERCEPTION OF ELECTRONIC COMMUNICATIONS

Application under penalty of perjury having been made before me by ________, an "Investigative or Law Enforcement Officer" as defined in Section 2510(7) of Title 18, United States Code, and an "attorney for the Government" as defined in Rule 54(c) of the Federal Rules of Criminal Procedure, for an order authorizing the interception of electronic communications pursuant to Section 2518 of Title 18, United States Code, and full consideration having been given to the matters set forth therein, the court finds:

A. There is probable cause to believe that ____________ ____________ and others as yet unknown, have committed and are committing felony offenses in violation of Section(s) ________________of Title ____________of the United States Code.

B. There is probable cause to believe that particular electronic communications concerning the offenses listed herein will be obtained through the interception for which authorization is herewith applied. In particular, these electronic

FORM 4

communications will concern the (<u>characterize offenses</u>) In addition, the communications are expected to constitute admissible evidence of the commission of the aforementioned offenses.

C. Normal investigative procedures either have been tried without success, reasonably appear unlikely to succeed if tried, or would be too dangerous.

D. There is probable cause to believe that the electronics communications facilit(ies)(y), ______________________________ owned or leased and operated by ______________________________ and located in the premises known as __________________________ (has), (have) been and (is) (are) being used by ______________ ____________________ and others as yet unknown in connection with the commission of the above stated offenses.

WHEREFORE, IT IS HEREBY ORDERED that the <u>(investigative agency)</u> is authorized, pursuant to an application authorized by <u>(name of applicant</u>) pursuant to the authority vested in him by Section 2516(3) of Title 18, United States Code: to intercept electronic communications of ________________ and others as yet unknown, concerning the above described offenses to and from ______________________________________ and located in the premises known as ______________________________. Such interception shall not automatically terminate when the type of communications described above in paragraph (B) have first been obtained but shall continue until communications are intercepted that reveal the manner in which ________________ and others as yet unknown, participate in the specified offenses and that reveal the identities of (his) (her) (their) co-conspirators, their places of operation, and the nature of the conspiracy involved therein, or for a period of (not to exceed 30) days, whichever is earlier; pursuant to Section 2518(5) of Title 18, United States Code, the time set forth in this order shall run from the earlier of the day on which the investigative or law enforcement officer first begins to conduct the interception or ten days from the date of this order.

Providing that, this authorization to intercept electronic communications shall be executed as soon as practicable after the signing of this order and shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under Chapter 119 of Title 18 of the United States Code, and must terminate upon attainment of the authorized objective or, in any event, at the end of (not to exceed 30) days measured from the earlier of the day on which the investigative or law enforcement officer first begins to conduct the interception or ten days from the date of the order, whichever is earlier.

Providing also, that applicant shall provide the court with a report on or about (such intervals as the court may require) days following the date of this order showing what progress has been made toward achievement of the authorized objective and the need for continued interception.

Judge

Date

Akhil ~~AMAT~~ Amar
Yale law
202 432 — 4838
Yale law school [illegible]

KATZ (5?)

WIRE OR ELECTRONIC COMMUNICATION SERVICE PROVIDER

ORDER

This matter having come before the Court pursuant to the application of the United States for the interception of (wire)(electronic) communications on (facilities)(telephone numbers) ________________________ and subscribed to by ____________________________ at __________________________________.

IT APPEARING that the Court, having reviewed the application and having found that it conforms in all respects to the requirements of Title 18, United States Code, Sections 2516 and 2518, has this ____________ day of _________________, 19 _______, signed an Order conforming to the provisions of Title 18, United States Code, Section 2518, authorizing special agents of the (investigative agency) to accomplish the aforesaid interception, and

IT FURTHER APPEARING THAT (name of wire or electronic communication service provider) is a provider of electronic communication services within the meaning of Title 18, United States Code, Section 2510(15), and

IT FURTHER APPEARING that the applicant has requested that (name of wire or electronic communication service provider)

FORM 9

Subject: thanks!
Date: Mon, 10 Jul 2000 21:36:06 -0400
From: Joshua_S._Gottheimer@who.eop.gov
To: aedmonds1@home.com

1

Draft 07/10/00 9:30pm
Gottheimer/ Swire

CHIEF OF STAFF JOHN PODESTA
REMARKS TO PRESS CLUB ON ELECTRONIC WIRETAPPING
WASHINGTON, DC
July 14, 2000

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn?t even imagined just a few years before.

Morse?s invention set in a motion a technological revolution that would forever change the way man would communicate. Only a few years later, in 1858, Queen Victoria bridged the waters of the Atlantic, when she sent the first transatlantic telegraph to President Buchanan in the White House. Just two decades later, using a funnel, a cup of acid, and some copper wire, Alexander Graham Bell invented a device to give voice -- not just words ? a way to travel.

the remarkable

Today, the great revolution in communication technology continues. >From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with same access to a reservoir of information ? from Shakespeare?s first sonnet to the remarkable photos just taken of Mars.

The Internet, like Morse?s telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values ? and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information ? from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has taken steps to keep our laws and policies in line with the latest advances in technology. To combat cyber-terrorism, we?ve introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. Just this February, in his Cyber Security Summit, the President ~~emphasized the~~ ensuring role and responsibility of the private sector in ~~implementing~~ computer and network security. We?ve also worked to develop strong encryption tools ? like those ~~implemented in~~ put in place by the European Union -- to provide tighter security and privacy in election communications.

Additionally, we?ve taken steps to ensure that the appropriate cyber security measures are included as part of all government computer systems. (2) Unfortunately, Congress has not given us the necessary funding the President has requested to take additional steps, such as funding an internal expert review team. (1) ~~And~~ We?ve taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens.

2

Supreme Court Justice Louis Brandies once said, ?Time works changes ? [it] brings into existence new conditions and purposes.? Today I want to talk to you about another step we should take to keep our laws consistent with the latest advances: the updating of existing wiretap laws. At the heart of the issue is the Fourth Amendment, which states that, ?The right of the people be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.?

In 1787, a person?s most important ?papers and effects? -- like diaries and letters -- were almost undoubtedly in their home or place of business. These papers were protected by the requirement of a warrant before the state could enter and search. But over time, with advances in technology, people no longer relied solely on paper and pen to communicate with one another. By the turn of the 20th Century, people were using the telephone for personal calls and business transactions. By the 1980s, Americans were using e-mail. These advances in technology have forced an ongoing debate in Congress and in the Courts over the application of the Fourth Amendment.

In the 1928 Olmstead case, the Supreme Court found that conversations over the telephone were not protected by the Fourth Amendment, and therefore wiretapped conversation could submitted as evidence. Judge Brandeis disagreed and argued that, ?There is, in essence, no difference between the sealed the letter and private telephone message.? Wiretaps of phones, Brandeis argued, invaded the privacy of people on both ends of the line ? the same privacy the framers intended to protect with the Fourth Amendment.

The 1968 Court agreed with Brandeis, when it ruled in Katz vs. the United States that an individual?s phone conversation was protected by the Fourth Amendment, and therefore inadmissible in court proceedings. Later that year, Congress responded to the Court?s decision by passing new legislation with strict standards for all wiretaps.

Title III of the 1968 Crime Control and Safe Streets Act required a court order and high-level Justice Department approval for all phone wiretaps. It only allowed wiretaps in the most serious crimes, such as espionage, treason, and crimes of violence. And, in those cases, it required detailed annual reports on the number and nature of all taps. Most significantly, Title III ruled that any information attained outside the parameters of the law was inadmissible in court.

Title III remained relatively untouched until the mid-1980s, when cellular telephone service, e-mail, and other computer-to-computer communication put new demands on the 1968 law. Title III of the 1968 law only applied to wire and voice communications ? not to wireless phone conversations or e-mail. But by 1984, there were more than 7,000 Americans using cellular phones, and more than 400,000 logging onto electronic mail.

In response, under the leadership of Senator Leahy, Congress adopted the Electronic Communications Privacy Act of 1986 -- once again updating its laws to keep pace with changing technology. Before ECPA, the government could use an electronic wiretap to monitor an individual?s e-mails with a mere subpoena. ECPA changed that, and put in place many of the protections the courts had given to phone conversations two decades earlier.

ECPA did several things: it made clear that wireless voice communications were covered to the same degree as wireless voice communications. It extended some, but not all, privacy protections to electronic communications intercepted in real-time. It set standards for access to stored e-mail and other electronic communications, and it adopted the trap and trace statute, governing real-time ?interception? of ?numbers dialed on a phone line.? ECPA also made it a federal crime to intercept electronic mail, data transmission and other electronic communications. This legislation was a big step, and one that was sorely needed with the advent of electronic communication.

Today, ECPA ? like its predecessors ? has, in many ways, become outdated by new advances in computer technology and electronic communication. Our country, and the world, is increasingly more digital ? increasingly more interactive. Since the passage of ECPA, we?ve seen a communications revolution with the rise of the cell phone and the development and use of the World Wide Web.

Today there are more 360 million cell phone users, and more than 50 million households online in the United States. That?s an increase of more than 1250% since 1984 alone. More than over 1.4 billion e-mails changes hands each and every day. Computer users today send e-mail from their home phone lines through Internet Service Providers, and they download files and e-mails onto shared servers at work. A growing number of Americans ? 2.2 million ? log on to the Internet and send e-mail through cable modems -- a means of connection that wasn?t even considered when ECPA was written.

ECPA was not devised to address many of the issues related to these newer, faster means of electronic communication. It doesn?t extend Title III protections to email sitting on the server of an Internet Service Provider ? like those in Yahoo?s corporate headquarters in Santa Clara, California. It doesn?t include other essential provisions ? like the scope of crimes covered ... and the need for Justice Department approval. And ECPA doesn?t include a statutory suppression rule for government violations, or a mandate for annual reports.

What does this mean? It means that data stored on networks is not afforded full privacy protection. That many of the protections in the wiretap law do not apply to email and other Internet services Americans often use. It means that ISP customers are not entitled to notice when personal information is subpoenaed in civil lawsuits. And it means that inconsistent standards apply to government access to information.

Basically, the same e-mail sent different ways ? through cable, phone lines, or an ISP -- is subject to different privacy standards. Considering the extent to which our electronic correspondence contains our most sensitive thoughts and information -- shouldn?t they count as the ?papers and effects? mentioned in the Fourth Amendment? It?s time to adopt legislative protections that map Fourth Amendment principles onto the latest technology. It?s time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations.

I propose the following legislative actions:

First, some current statutes apply to ~~criminal~~ criminals who use hardware ?devices? but not to identical crimes that use software instead. Such telephone-era laws should be clearly updated to apply to an Internet era where hardware and software are interchangeable. One of our Administration?s central principles has been technology neutrality -- the idea that the government and the laws should be generally neutral between different technologies. In our proposed legislation, we would amend statutes that are hardware-specific or use ?devices? and other outmoded language. We would also continue to study ~~whether~~ any additional legislative responses are appropriate to distributed denial-of-service or other new threats.

Second, we need to achieve Parity in the way ~~harmonization of how~~ the laws apply to different forms of communication. As I mentioned, the current law sets stricter standards for law enforcement access to ?wire? communications such as telephone calls than for ?electronic? communications such as e-mail. The market should play the central role in picking technological winners and losers, not Congress or the regulators they do to

In order to achieve this neutrality, we propose to harmonize the legal standards that apply to law enforcement access to e-mails, telephone calls, and cable services. For more than 30 years, federal law has set a tough, but manageable standard for when law enforcement officers can listen to the contents of phone calls. Today, the same legal protections should apply ~~to~~ equally to electronic communication as telephone communication. These protections include high-level approval within the Department of Justice, use ~~only~~ for only the most serious crimes, and suppression of evidence in court if the rules are not ~~followed.~~ the need for the advice ?

At the same time, we propose to change the standards that apply to cable services. Under the current Cable Act, even where there is clear proof of serious crimes, law enforcement officials cannot gain access to subscriber records -- unless the customer first can contest the issue in court. With our proposal, we would retain the underlying purpose of the Cable Act to keep confidential the list of shows that a customer has watched. But, when cable systems are used to access the Internet, we believe the rules should be the tough but manageable standards we also support for e-mails and telephone calls.

Third, we need to seek balance among crucial goals -- including the protection of public safety, the achievement of economic growth and digital opportunity, and the preservation of privacy and civil liberties. That?s a challenge that our forefathers grappled with when they wrote the Constitution, and one that our government and courts have struggled with ever since. Our aim should be to enhance law enforcement authorities ability to address unlawful conduct, but also to enhance privacy and civil liberties on the Internet.

For example, we need to update the longstanding legal rules that govern when law enforcement can track the identity of those with whom we communicate. Our ?trap and trace? rules come from the era of the traditional telephone network, when one company offered nationwide phone service. Telephone service today is offered by a bewildering variety of companies that offer local, long distance, and wireless services. Tracing a phone call often requires separate subpoenas in the various courts where each of the companies operates. The problem in tracing Internet communications to their source can be even worse. The structure of the Internet means that communications are routinely shuttled among many nodes, often in different federal court districts.

Today, we are proposing ways to make these "trap and trace" rules more effective for law enforcement, while also better assuring privacy and civil liberties. We believe that a federal court should be able to issue one order to trace a communication to its source, and that order should be effective nationwide. We also believe that there should be greater judicial oversight of trap and trace authorities. Federal law should make clear that such orders should only be issued after a judicial officer has determined that the proper factual showing has been made.

In the early years of our republic, Thomas Jefferson said, ?America?s institutions must move forward hand-in-hand with the progress of the human mind.? Today, the progress of the human mind is certainly racing forward at break-neck speech. Technology is opening up a new world of possibility -- but it is also challenging our privacy in ways we might never have imagined. In the right hands, the computer has become an indispensable tool for education, business, research and development. But in criminal hands, the same computer becomes a tool of destruction. As in any era of great progress, we must work together to ensure that our democracy and our laws keep pace with our minds -- and that we protect our civil liberties, not just the law enforcement mechanisms that were instituted to preserve them.

electronic

messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has taken steps to keep our laws and policies in line with the latest advances in technology. To combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. Just this February, in his Cyber Security Summit, the President emphasized the role and responsibility of the private sector in ensuring computer and network security. We've also worked to develop strong encryption tools – like those put in place by the European Union -- to provide tighter security and privacy in election communications.

Additionally, we've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And we've taken steps to ensure that the appropriate cyber security measures are included as part of all government computer systems. Unfortunately, Congress has not given us the necessary funding the President has requested to take additional steps, such as funding an internal expert review team.

Supreme Court Justice Louis Brandies once said, "Time works changes ... [it] brings into existence new conditions and purposes." Today I want to talk to you about another step we should take to keep our laws consistent with the latest advances: the updating of existing wiretap laws. At the heart of the issue is the Fourth Amendment, which states that, "The right of the people be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

In 1787, a person's most important "papers and effects" -- like diaries and letters -- were almost undoubtedly in their home or place of business. These papers were protected by the requirement of a warrant before the state could enter and search. But over time, with advances in technology, people no longer relied solely on paper and pen to communicate with one another. By the turn of the 20th Century, people were using the telephone for personal calls and business transactions. By the 1980s, Americans were using e-mail. These advances in technology have forced an ongoing debate in Congress and in the Courts over the application of the Fourth Amendment.

be

In the 1928 *Olmstead* case, the Supreme Court found that conversations over the telephone were not protected by the Fourth Amendment, and therefore wiretapped conversation could submitted as evidence. Judge Brandeis disagreed and argued that, "There is, in essence, no difference between the sealed the letter and private telephone message." Wiretaps of phones, Brandeis argued, invaded the privacy of people on both ends of the line – the same privacy the framers intended to protect with the Fourth Amendment.

The 1968 Court agreed with Brandeis, when it ruled in *Katz vs. the United States* that an individual's phone conversation was protected by the Fourth Amendment, and therefore inadmissible in court proceedings. Later that year, Congress responded to the Court's decision by passing new legislation with strict standards for all wiretaps.

At the same time, we propose to change the standards that apply to cable services. Under the current Cable Act, even where there is clear proof of serious crimes, law enforcement officials cannot gain access to subscriber records -- unless the customer first can contest the issue in court. With our proposal, we would retain the underlying purpose of the Cable Act to keep confidential the list of shows that a customer has watched. But, when cable systems are used to access the Internet, we believe the rules should be the tough but manageable standards we also support for e-mails and telephone calls.

Third, we need to seek *balance* among crucial goals -- including the protection of public safety, the achievement of economic growth and digital opportunity, and the preservation of privacy and civil liberties. That's a challenge that our forefathers grappled with when they wrote the Constitution, and one that our government and courts have struggled with ever since. Our aim should be to enhance law enforcement authorities ability to address unlawful conduct, but also to enhance privacy and civil liberties on the Internet.

For example, we need to update the longstanding legal rules that govern when law enforcement can track the identity of those with whom we communicate. Our "trap and trace" rules come from the era of the traditional telephone network, when one company offered nationwide phone service. Telephone service today is offered by a bewildering variety of companies that offer local, long distance, and wireless services. Tracing a phone call often requires separate subpoenas in the various courts where each of the companies operates. The problem in tracing Internet communications to their source can be even worse. The structure of the Internet means that communications are routinely shuttled among many nodes, often in different federal court districts.

Today, we are proposing ways to make these "trap and trace" rules more effective for law enforcement, while also better assuring privacy and civil liberties. We believe that a federal court should be able to issue one order to trace a communication to its source, and that order should be effective nationwide. We also believe that there should be greater judicial oversight of trap and trace authorities. Federal law should make clear that such orders should only be issued after a judicial officer has determined that the proper factual showing has been made.

In the early years of our republic, Thomas Jefferson said, "America's institutions must move forward hand-in-hand with the progress of the human mind." Today, the progress of the human mind is certainly racing forward at break-neck speech. Technology is opening up a new world of possibility -- but it is also challenging our privacy in ways we might never have imagined. In the right hands, the computer has become an indispensable tool for education, business, research and development. But in criminal hands, the same computer becomes a tool of destruction. As in any era of great progress, we must work together to ensure that our democracy and our laws keep pace with our minds -- and that we protect our civil liberties, not just the law enforcement mechanisms that were instituted to preserve them. Thank you .

Korea Economic Weekly May 1, 2000

Korea Economic Weekly

May 1, 2000

SECTION: BUSINESS; No. 586

LENGTH: 187 words

HEADLINE: Samsung develops advanced TFT-LCD for cellular phones

BODY:

Samsung Electronics has developed an advanced thin-film-transistor liquid crystal display (TFT-LCD) for cellular phones.

The company announced on April 23 that it has developed the new TFT-LCD for IMT-2000, designed to provide ultra-high resolution for moving or still images.

The new product has 720 (horizontal) by 240 (vertical) pixels, making its resolution four times higher than that of Japanese competitors. In addition, its power consumption stands at a third of existing displays because of a built-in reflecting plate.

Samsung will begin to mass-produce the TFT-LCDs for IMT-2000 in the latter half of this year and begin exports to oversea markets by the year's end.

The **number of cellular phone users** throughout the world is estimated to reach 360 million this year and rise to 1.6 billion by 2005, an official of Samsung Electronics forecast.

The number of hand-held terminals with TFT-LCD panels is estimated to reach 3.57 million this year and to dramatically rise to 375 million by 2005, accounting for 23 percent of the total hand-held telephonic devices of the world, he added.

LANGUAGE: ENGLISH

LOAD-DATE: April 28, 2000

During the intervening years, both the benefits and risks from widespread use of electronic communications have fundamentally changed. On the benefit side, we have seen all the many advantages that come from having information flows become global, instantaneous, and far less expensive. The Internet has become an engine for education, entertainment, and economic growth. Individuals and businesses now entrust a much greater portion of their most sensitive information to e-mail and other electronic communications.

On the risk side, however, there is no doubt that criminal, terrorist, and other unlawful activity is increasingly moving to the Net. As law enforcement and national security agencies confront these threats, some of the old statutory language simply does not apply to new technology. For example, some current statutes apply to criminals who use hardware "devices" but not to identical crimes that use software instead. Such telephone-era laws should clearly be updated to apply to an Internet era where hardware and software are often interchangeable. In proposed legislation, we should amend statutes that are hardware-specific or use "devices" and other outmoded language. We will also continue to study whether any additional legislative responses are appropriate to distributed denial-of-service or other new threats.

A second theme is to achieve *harmonization* of how the laws apply to different forms of communication. Current law, for instance, sets stricter standards for law enforcement access to "wire" communications such as telephone calls than for "electronic" communications such as e-mail. Whether or not such a difference made sense when it was enacted in 1986, the separate standards are much harder to justify today when industries have converged and many telephone calls are actually completed through the Internet. Similarly, for Internet communications, the rules may differ substantially depending on whether homeowners get to the Internet via a dial-up phone service, a cable provider, or a satellite service. In our era of rapid technological change, one of the Administration's central principles has been *technology neutrality* -- the idea that the government and the laws should be generally neutral between different technologies such as different sorts of Internet service providers. The market should play the central role in picking technological winners and losers, not Congress or the regulators.

In order to achieve this neutrality, we propose to harmonize the legal standards that apply to law enforcement access to e-mails, telephone calls, and cable services. For over 30 years, federal law has set a tough but manageable standard for when law enforcement officers can listen to the contents of phone calls. Today, when e-mail and other "electronic" communications are relied upon similarly to phone calls, we believe that the same legal protections should apply. These protections include high-level approval within the Department of Justice, use only for the most serious crimes, and suppression of evidence in court if the rules are not followed.

At the same time, we propose to change the standards that apply to cable services. Under the current Cable Act, even where there is clear proof of serious crimes, law enforcement officials cannot gain access to subscriber records unless the customer first can contest the issue in court. We would retain the underlying purpose of the Cable Act to keep confidential the list of shows that a customer has watched. But, when cable systems are used to access the Internet, we believe the rules should be the tough but manageable standards we also support for e-mails and telephone calls.

The third theme for law enforcement authorities is to seek *balance* among crucial goals including protection of public safety, achievement of economic growth and digital opportunity, and preservation of privacy and civil liberties. The President emphasized this need for balance in his remarks at the February Cyber Security Summit. [Perhaps add quotes from POTUS or Podesta at that event.] Our aim should be to enhance law enforcement authorities to address unlawful conduct and also to enhance privacy and civil liberties on the Internet.

An example of how to achieve all of these goals concerns the longstanding legal rules that govern when law enforcement can track the identity of those with whom we communicate. Today, we are proposing ways to make these "trap and trace" rules more effective for law enforcement while also better assuring privacy and civil liberties.

Our "trap and trace" rules come from the era of the traditional telephone network, when one company offered nationwide phone service. In that setting, a federal subpoena to determine a caller's identity could be served on the one company and have effect nationwide. By contrast, telephone service today is offered by a bewildering variety of companies that offer local, long distance, and wireless services. Tracing a phone call may require separate subpoenas in the various courts where each of the companies operates. The problem in tracing Internet communications to their source can be even worse. The structure of the Internet means that communications are routinely shuttled among many nodes, often in different federal court districts.

To *update* the "trap and trace" rules for these changed circumstances, the Administration believes that a federal court should be able to issue one order to trace a communication to its source, and that order should be effective nationwide. At the same time that we make nationwide enforcement more effective, we also should provide greater judicial oversight of trap and trace authorities. Federal law should make clear that such orders should issue only have after a judicial officer has determined that the proper factual showing has been made.

[Developing options for additional issues that may be included.]

[Closing paragraphs. Here are some free quotes on privacy and civil liberties that we could use if appropriate:

"Civil liberties had their origin and must find their ultimate guaranty in the faith of the people." Justice Robert Jackson, Douglas v. Jeannette, 319 U.S 157 182 (1943). This quote could bolster the idea that we need statutory implementation of 4th Amendment values when the Constitution itself does not apply.

"The right to be alone -- the most comprehensive of rights, and the right most valued by civilized

Quotation Collection: Thomas Jefferson

Author Menu | Topic Menu

"That government is best which governs the least, because its people discipline themselves."

"It is more honorable to repair a wrong than to persist in it."
-- To the Cherokee Chiefs, January 10, 1806

"We often repent of what we have said, but never, never, of that which we have not."

"Laws are made for men of ordinary understanding, and should therefore be construed by the ordinary rules of common sense. Their meaning is not to be sought for in metaphysical subtleties, which may make anything mean everything or nothing, at pleasure."
-- Letter, William Johnson, 1823

"I like the dreams of the future better than the history of the past."
-- Letter, John Adams, 1816

"The execution of the laws is more important than the making of them."
-- Letter, Abbe Arnond, 1789

"Integrity of views more than their soundness, is the basis of esteem."
-- Letter, Elbridge Gerry, April 22, 1800

56-Kbps modems, will likely help crowd out 33.6-Kbps modems. The modem with the shortest run was the 9.6-Kbps **modem, introduced in** 1989 and displaced within 18 months by the 14.4-Kbps modems released in 1991.

LANGUAGE: ENGLISH

LOAD-DATE: March 31, 1998

Mickey Ibarra
07/10/2000 07:20:10 AM

Record Type: Record

To: Joshua S. Gottheimer/WHO/EOP@EOP

cc: Seth J. Applebaum/WHO/EOP@EOP, Zina C. Pierre/WHO/EOP@EOP
Subject: Re: DRAFT--NACO Video. Comments pls to Gottheimer ASAP 62554.

Josh, these remarks are good. Only two changes I suggest in the firs paragraph. Please add an acknowledgment of Vernon Gray, president of NACo. He is a proven friend of our Administration. Also, rather than saying "As the only organization," I suggest "As an organization dedicated to representing". (The County Executives of America would argue that they also represent counties.) Thanks.

Lowell A. Weiss
06/25/2000 07:38:00 PM

Record Type: Record

To: See the distribution list at the bottom of this message

cc:
Subject: genome -- 7:00pm

Draft 6/25/00 7:00pm
Lowell Weiss

PRESIDENT WILLIAM J. CLINTON
REMARKS ON MILESTONE IN HUMAN GENOMICS
THE EAST ROOM
June 26, 2000

Acknowledge: P.M. Blair, who will join us via live teleconference in a moment; Ambassadors from [the U.K.], Japan, [Germany], France, [China] – whose scientists have contributed mightily to the vast international consortium that is the Human Genome Project; Sec. Shalala, who could not be here today, Sec. Richardson, Dr. Ruth Kirschstein, Dr. Ari Patrinos, and the scientists of the Dept. of Health and Human Services and the Dept. of Energy who have played such an important part of the Human Genome Project since its inception; Dr. Neal Lane; Dr. Francis Collins, the director of the international Human Genome Project; Celera [sa-LAIR-ah] Pres. Dr. Craig Venter; Sens. Domenici, Harkin, Sarbanes; other distinguished guests.

Nearly two centuries ago, Thomas Jefferson and a trusted aide spread out a magnificent map upon this very floor – a map that Jefferson had long prayed he would behold within his lifetime. The aide was Meriwether Lewis – and the map was the product of Lewis's courageous expedition across the young American nation. It was a map that defined the contours of a continent and forever expanded the frontiers of our imagination.

Today, the world is joining us here in the East Room to behold a map of even greater significance: We are here to celebrate the completion of the first survey of the entire human genome. Without a doubt, this is the most important, most wondrous map ever produced by humankind. It is the map of life itself.

This moment we are here to witness was brought about through the brilliant and painstaking work of scientists all over the world, including many of the men and women who are here today. It was not even 50 years ago that a young Englishman by the name of Crick and a brash, even younger American named Watson first discovered the elegant helical structure of our genetic code. Dr. Watson [*present in the audience*], from this vantage point, the way you announced your discovery in the journal *Nature* seems almost quaint: "This structure has novel features which are of considerable biological interest." That was one of the greatest understatements of all time.

How extraordinarily far we have traveled since that day of fundamental discovery. In the intervening years, we have pooled the combined wisdom of biology, chemistry, physics, engineering, mathematics, and computer science. We have tapped the great strengths and insights of the public and private sectors. More than a thousand researchers across six nations have revealed nearly all 3 billion letters of our miraculous genetic code. I congratulate all of you on your stunning, humbling achievement.

I believe today's announcement represents more than just an epoch-making triumph of science and reason. After all, when Galileo discovered that he could use the tools of mathematics and mechanics to understand the motion of celestial bodies, he felt, in the words of one eminent researcher, that he had learned "the language in which God created the universe." Today, we are learning the language in which God created life. We are gaining ever more awe for the complexity, the beauty, the wonder of God's most divine and sacred gift.

With this profound new knowledge, humankind is on the verge of gaining immense new power to heal. Genome science will have a real impact on all our lives. It will revolutionize the diagnosis, prevention, and treatment of most, if not all, human disease. In the coming years, doctors will increasingly be able to cure diseases like Alzheimer's, Parkinson's, diabetes, and cancer by attacking their genetic roots. Just to offer one example, patients with some forms of leukemia and breast cancer are already being treated in clinical trials with sophisticated new drugs that precisely target the faulty genes in cancer cells, with little or no risk to healthy cells. In fact, it is now conceivable that our children's children will know the term "cancer" only as a constellation of stars.

But today's historic achievement is only a marvelous starting point. There is much hard work that remains to be done. And that is why I am so pleased to announce that from this moment forward, the robust and healthy competition that has led us to this day - and is always essential to the progress of science - will be coupled with an enhanced spirit of public-private cooperation.

Public and private research teams are committed to publishing their genomic data simultaneously later this year, for the benefit of researchers in every corner of the globe. And after publication, both sets of teams will join together for an historic sequence-analysis conference. Together, they will examine what scientific insights have been gleaned from both efforts - and how we can most judiciously proceed toward the next majestic horizons.

And what are those next horizons? Well, first, we will complete a virtually-error-free <u>final</u> draft of the human genome before the 50th anniversary of the discovery of the double helix, less than three years from now. Second, through sustained and vigorous support for public and private research, we must sort through this trove of genomic data to identify <u>every</u>

human gene; we must discover the function of these genes and their protein products; and then we must rapidly convert that knowledge into treatments that can lengthen and enrich our lives.

I want to emphasize that the biotechnology and pharmaceutical industries are absolutely essential to this endeavor. For it is they who will bring to market the life-enhancing applications of the information from the human genome. And for that reason, this Administration is committed to helping them to make the kind of long-term investments that will change the face of medicine forever.

The third horizon that lies before us is one that science cannot approach alone. It is the horizon that represents the ethical, moral, and spiritual dimension of the power we now possess. We must not shrink from exploring the far frontiers of science. But as we consider how to use new discoveries, we must also not retreat from our oldest and most cherished human values.

We must ensure that new genome science and its benefits will be directed toward making life better for all citizens of the world – never just a privileged few. As we unlock the secrets of the human genome, we must work simultaneously to ensure that new discoveries never pry open the protective doors of privacy. And we must guarantee that genetic information cannot be used to stigmatize or discriminate against any individual or group. Increasing knowledge of the human genome must never change the basic belief upon which our ethics, our government, our society are founded: All of us are created equal, entitled to equal treatment under the law.

After all, I believe that one of the great truths to emerge from this triumphant expedition inside the human genome is that in genetic terms all human beings, regardless of race, are more than 99.9 percent the same. What that means, my friends, is that modern science has confirmed what we always learned from ancient faiths: the most important fact of life on this Earth is our common humanity. My greatest wish on this day for the ages is that this incandescent truth will always guide our actions as we continue to march forth into this, the greatest age of discovery ever known.

And now, it is my great pleasure to turn to my good friend Prime Minister Tony Blair, who is joined in the State Dining Room at 10 Downing Street by Dr. Fred Sanger and other world-renowned scientists. With the generous support of the Wellcome Trust, British scientists have played an invaluable role in reaching this milestone. On behalf of the American people, I would like to thank the British nation for the brilliant work that you have brought to this international effort.

And Mr. Prime Minister, I would like to salute not only your unwavering support for genome research but also your visionary commitment to sparking ever-greater innovation across the full spectrum of science and technology. On a personal note, I can't help but think that the year of your son's birth will always be remembered for the remarkable achievements we are announcing today.

*[YOU should remain at the lectern while P.M. Blair makes his remarks. After he completes his formal remarks, **YOU** will briefly converse with him.]*

[Proposed brief, conversational remarks to P.M. Blair:]

Tony, I would like to pick up on your last remark – about safeguarding our shared values in this new age. I believe that the Human Genome Project is the single most important international scientific expedition ever undertaken. And as we move forward, I would like to see the U.S., the U.K., and many other nations join together in the same focused way to broaden our dialogue on the ethical, legal, and social implications of this expedition. After all, these implications cross every possible discipline and every possible divide.

[At the conclusion of your brief conversation with P.M. Blair, YOU will say a brief word about Dr. Craig Venter and introduce Dr. Francis Collins.]

In a few moments we will hear from Celera Pres. Dr. Craig Venter, who shares in the glory of this day thanks to his visionary pursuit of innovative strategies to sequence the human genome as rapidly as possible.

But before we do, I would like invite Dr. Francis Collins to the lectern and congratulate him on his remarkable accomplishments. From his development of some of the central methods for finding human disease genes, to his successful application of those methods to the discovery of the cystic fibrosis gene in 1989, to his current leadership of the international Human Genome Project, he has combined talents in rigorous science and a profound sensitivity to ethical, legal, and social issues. He is a physician-scientist of great faith, compassion, energy, and integrity. And more than any other American, he has helped us to understand how the marvels of genome science will improve human health. Dr. Collins...

*[After Dr. Collins and Dr. Venter conclude their remarks, **YOU** will return to the lectern to make brief closing remarks.]*

# # #

Message Sent To:____

the/a

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With touch of a finger, he broke down geographic barriers that had long kept us apart, opening up a world of a possiblity that was never even imagined just a few years before.

Morse's invention set in a motion a technological revolution that would forever change the way man would communicate. Only a few years later, in 1858, Queen Victoria bridged the waters of the Atlantic, when she sent the first transatlantic telegraph to President Buchanan in the White House. Just two decades later, using a funnel, a cup of acid, and some copper wire, Alexander Graham Bell invented a device to give a person's voice -- not just his words -- a way to travel.

Today, the great American revolution in technology continues. From small towns to big cities, the Internet is brining millions of people closer, giving them new ways to find information and to stay in touch. When it was ~~in~~vented just thirty years ago, there were just two computers exhanging very simple messages. Now there are almost 50 million households online, all with the access to the same information.

~~computers, it has~~ now grown But like Morse invention did more than a century a half ago, advances in science and technology bring w/ them a host of new and exciting challenges the invention of the telegraph also posed/ introduced a world of new challenges to the way we lived, and the to laws we lived by. We have sought to live w/ these challenges.

Most importantly, he set in a motion a technological revolution that would lead to first

the first he changed the way man would communicate for the rest of time. While – changing the way man would communicate for the ropening the gates to a world of communication from This is a great time to be alive in America. The Internet is ... a revolution in technology is underway. It's more than a time of innovation, it's a time of fundamental transformation, the kind that happens, at most, every hundred years. Last month, we celebrated the completion of the first survey of the entire human genome/ Last month, we announced a major breakthrough in human genome research which could eradicate many of the most deadly diseases. Last month, the President signed into law the Electronic Signatures Act, which gives online contracts the same legal force as equivalent paper contracts.

Technology is changing so rapidly – key is to keep our laws and our government in synch with our progress
Great potential/ progress/ discovery also brings great responsibility, new challenges. Just last week discovered human genome – [see genome speech]. That's something that our country and our courts have responded to since our founding, and it's something we will continue to do as we evolve as a nation. Over the last 7 years, w/ the advances medicine and technology, we've done x, y, z.

Our admin has worked hard to keep up w/ our progress (in may … ea michigan commencement, medical privacy, signed eo …) … as judge brandeis said, " update our laws"

We know that we have to make cyberspace open and free. We have to make, at the same time, computer networks more secure and resilient, and we have to do more to protect privacy and civil liberties.

One area that's always been at the forefront of concern has been privacy (4th amendment privacy principles). Particularly true w/ laws that directly relate to our civil liberties – law enforcement (balance), and wire tapping. Historically been a 4th amendment issue, which states X. key has always been balance: between public good and civil liberties.

In updating enduring constitutional values for the computer age, we need to assure that our citizens' personal data and communications are appropriately protected.

We recognize that information technology is changing rapidly and constantly providing both new security capabilities and challenges. We will never reach a "perfect solution."

Original intent of forefathers

Here of course technology is always changing.
In the 18XX… the threshold for invasion privacy – protection privacy, home, diary … assume whether or not in a sphere of privacy.

Over time it has been updated:
In 1920, when first seminal case on tapping heard – olmstead. At that time, only

In 1968, … time of the case … law changed. Katz said x … Focused on phone, although there were websites at the time. Title III out of that. Email.

In 1986, … something I worked on closely … cell phones … passed x law to keep up w/ nascent web … ECPA. Forward looking at the time.
That law says:

But now – times have indeed changed again. We need to change w/ them, like our forefather did, and at other seminal moments in our history. Since 1986, x websites have been created. More than 2.2M cable modem subscribers. Then there were only 50… now over 50M. But the law still says x. It's easier today for fed officials to gain access to my grandmother's cookie recipe she sent me on aol, than a terrorists master mind plan sent on his cable modem. Cable law from 1984 says 10 days. Don't need x, y, …

Law enfrocment may obtain the legal authority to access a suspects' communications or dta
We need to update our law – harmonize them. So that equal laws for electronic tapping as wire tapping. so we can strike that balance – where cable not too difficult. Email not so easy. Privacy vs. law enforcement – so if drug, child porn.

We should update our laws so they do: x, y, z

Conclusion

In the early years of our republic, Thomas Jefferson said, "America's institutions must move forward hand-in-hand with the progress of the human mind." Today, the progress of the human mind is certainly racing forward at break-neck speech. We must work together to ensure that our democracy/ and our laws keep pace. "

Each of these examples was a pivotal episode in American history in which complex social, economic, and technological forces came together. Facing the challenges of the day, America's governmental, societal and technical leaders crafted a new vision of the future, and in the process became pioneers on a new frontier of opportunity and promise.

America now faces a new time of pivotal change, enormous opportunity, and promise. This time, technology itself presents both an opportunity and a threat to global society increasingly dependent on, and connected by, advanced computing and communications. Continuing a balanced strategy that advances our national interests is the challenge of our day.

2. Cyber America: Great Promise and Serious Risks

America now stands on the brink of revolution fueled by machines - computers - and networks of computers that facilitate the instant exchange of and access to ideas and information. The computer has and will continue to revolutionize virtually all aspects of American society, just as electricity, the power grid and the railroad changed our forefathers' society.

The Computer as an Economic Engine. It is well known that the computer, and its application in business, commerce, education and recreation has transformed the American economy. America is becoming a country of "knowledge workers," with the ubiquitous application of computer technology at its core. America's productivity today is grounded in computer applications and networks. Barcodes speed us through shopping lines and simultaneously facilitate store manager recordkeeping and reordering. Airline reservations can be booked from home computers. Everything from clothes to books to software can be purchased over the Internet. American companies are discarding their proprietary computer systems and using the Internet and the Web to increase productivity, network their entire chain of suppliers, and deliver "just-in-time" training to their employees. American students can conduct original research with colleagues on machines around the world with but a few keystrokes. Travelers can monitor current weather conditions in another country. Scientists can "conference" electronically and transmit astounding volumes of information in seconds to colleagues on other continents.

As remarkable as today's innovations are, the years ahead hold even greater promise. Computers will become virtual partners in all aspects of our lives. Homes will be centrally wired to allow integrated alarms, electronics, appliances, telephones, and computers to simplify our lives. Education will become more adaptive to the routines of individual students, and banking, finance, and shopping will increasingly migrate to the home and portable computing devices.

And in this process and through networking, computers have created the well-known "cyberspace" that eliminates the traditional boundaries of time and place and links governments, businesses, and individuals in the same electronic environment.

The Dangers of Cyberspace. Like any new tool in previous eras, computers can be used by those who prey on the innocent. International narcotics traffickers now routinely communicate with each other via computer messages. Hostile governments and even some transnational organizations are establishing cyber-warfare efforts, assigned the mission of crippling America's domestic infrastructure through computer attacks. Hackers destroy cyber-property by defacing homepages and maliciously manipulating private information. Pedophiles stalk unsuspecting children in computer chat rooms. Individuals post homepages with instructions to manufacture pipebombs, chemical weapons,

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release February 15, 2000

REMARKS BY THE PRESIDENT
IN PHOTO OPPORTUNITY WITH LEADERS
OF HIGH-TECH INDUSTRY
AND EXPERTS ON COMPUTER SECURITY

The Cabinet Room

11:57 A.M. EST

THE PRESIDENT: The room is smaller than it looks on television. (Laughter.) Usually I don't get so many of them coming in, except you guys are -- (laughter.)

Well, first of all, I want to welcome the leaders of the high-tech industry and experts on computer security to this meeting at the White House to talk about how to maximize the promise and minimize the risks to the Internet.

The disruptions at several websites last week highlight how important the Internet has become to our whole way of life in America, and how vulnerabilities at one place on the Net can create risks for all. Our administration has been working for years now to reduce vulnerabilities in government computers and to encourage the private sector to do more.

We know that we have to keep cyberspace open and free. We have to make, at the same time, computer networks more secure and resilient, and we have to do more to protect privacy and civil liberties. And we're here to work together.

Last month I released a draft plan to help do our part to meet these challenges. And in the budget I asked Congress for $2 billion for cyber security, to safeguard government networks, to detect attacks, to hire and train more security experts, to increase cooperation with the private sector. I want to jump-start this effort by providing $9 million right away to begin some of these key initiatives. And so we'll do what we can.

I understand that many leading industry members, including the companies represented here today, have agreed to create a mechanism to share cyber security information, and I applaud that. I am asking Secretary Daley and my Science Advisor, Dr. Neal Lane, and Richard Clarke from the White House, to work with these companies to accelerate our efforts with the private sector.

Now, having said that, and before we open the floor for questions, I'd like to ask Peter Solvik, who is to my right, the senior Vice President and chief information officer of CISCO Systems, to say a few words on behalf of the private sector people who are here today.

Peter.

MR. SOLVIK: Thank you, Mr. President. It is an honor for me to be here to discuss this important issue. First, I want to thank you and your team for working cooperatively with industry to pursue and

.d even biological agents. Crooks break into business computers, ither stealing funds directly or extorting payments from companies anxious to avoid more expensive disruption. Disgruntled employees, with valid access to their companies' system, can take steps to disrupt the business operations or steal proprietary, sensitive, and financial information. And our personal data is at risk of being unlawfully accessed and read by malicious individuals, without our knowledge, as it resides on or traverses communications and computer networks.

These concerns are not hypothetical. We have seen these types of activities, and other equally dangerous activity, in past and on-going cases. The danger posed by evil individuals using these powerful new tools grows by the day. Just as other technologies have the risk of being abused, it is necessary for us to evaluate how to respond. Without protective action, we will not be safe. America must take responsible steps to ensure that this promising electronic environment is safe for law abiding citizens and businesses.

3. Balancing America's Bedrock Values

While these problems seem unprecedented, in fact they represent a return to the bedrock problems faced by America's constitutional founders. American democracy became and remains a new experiment in government--balancing the rights of individuals against the imperatives of society and limiting the reach of government into personal, private lives, while mandating a government responsibility for public safety and security for all citizens.

Computers are now at the center of competing American values. In honest, law abiding citizens' hands, the computer becomes an indispensable tool for education, personal and commercial business, research and development, and communications. In criminal hands, the same computer becomes a tool of destruction and criminality.

Enter encryption. Over the past decade, another information technology has emerged that amplifies this tension - encryption. Encryption includes special instructions that scramble a clear readable message in complex ways that make it unreadable. For the strongest forms of encryption, only the intended recipient can unscramble the message and read the original plain text, unless someone else has gained access to the corresponding decoding software and decryption key.

Originally only available and used by military agencies, strong encryption is now available to many and has become a building block for the new digital economy. It is essential to provide security and privacy for electronic commerce and e-business. Encryption is critical because it allows individuals, businesses, and other organizations to share information privately without it being unlawfully intercepted or accessed by a third party, to establish their identities, and to maintain the integrity of information. Without the use of encryption, it is difficult to establish the trust that people and firms need to do business with each other, or to have confidence to run their business electronically. With the use of encryption:

- Individuals and consumers can securely conduct their finances and communicate with each other over the Web.

- Firms can transmit their software, music, movies, reports and other forms of intellectual property over the Internet while minimizing the risks of widespread piracy.

- Businesses can protect their company proprietary information over the Internet, with confidence that the information is secure from prying eyes.

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release February 15, 2000

Fact Sheet

Strengthening Cyber Security through Public-Private Partnership

Today the President and members of his Cabinet met with leaders of Internet and e-commerce companies, civil liberties organizations, and security experts to jointly announce actions strengthening Internet and computer network security. This meeting follows last month's release by the President of the National Plan for Information Systems Protection, which establishes the first-ever national strategy for protecting the nation's computer networks from deliberate attacks.

During today's meeting, industry executives announced their intention to join others to create an Internet industry mechanism to share information on cyber attacks, vulnerabilities and security practices to better respond to cyber-attacks and deliberate intrusions into computer networks. Recently, other industries such as banking and finance, and major telecommunications carriers, have created industry partnerships for cyber-security.

The President also announced immediate steps the government will take to strength security for our nation's computer systems:

Accelerated Spending on Cyber Security - A $9 million budget supplemental for Fiscal Year 2000, jump-starting key initiatives for cyber-security contained in the President's FY2001 $2 billion budget request for cyber-security. The request will accelerate new programs to educate Americans for cyber-security careers, build a system for protecting Federal government computers, and create a new Institute for Information Infrastructure Protection.

Research and Technology Development for Information Infrastructure Development - President Clinton supports federal government research and technology development for information infrastructure protection that the private sector does not have sufficient market incentives to generate on its own. The centerpiece of the federal government's efforts in this area will be the Institute for Information Infrastructure Protection (I3P), for which the President has requested $50 million in his Fiscal Year 2001 budget. The President has also requested a supplemental appropriation of $4 million for Fiscal Year 2000 to jumpstart the Institute's preparations. Science Advisor Neal Lane and NSC National Coordinator Dick Clarke will meet this Friday with members of the President's Committee of Advisors on Science and Technology and other computer security experts, research specialists, and industry leaders in an effort to help fill the gaps in the nation's research agenda for computer network security.

Partnership for Critical Infrastructure Security - Secretary Daley will participate in the first meeting of the Partnership for Critical Infrastructure Security next week to maximize cooperation between government and private sector initiatives for cyber-security. Since the vast majority of the United States' critical infrastructures are owned and operated by private industry, the Partnership recognizes and acknowledges that the Federal government alone cannot protect these infrastructures or assure the delivery of services over them. The Partnership will explore ways in which industry and government can jointly address the risks to the nation's critical infrastructures. It will provide a forum in which the various infrastructure sectors can meet to address issues relating to cross-sector interdependencies, explore common approaches and experiences, and engage other key professional and business communities that have an interest in infrastructure assurance. By doing so, the Partnership hopes to raise awareness, promote understanding, and, when appropriate, serve as a catalyst for action.

Private sector membership in the Partnership is open to infrastructure owners and operators; providers of infrastructure hardware, software, and services; risk management and investment professionals; and other members of the business community who are stakeholders in the critical infrastructures. Government representation will include state and local governments as well as Federal agencies and departments responsible for working with the critical infrastructure sectors and for providing functional support for the protection of those infrastructures.

###

Final 07/06/00 8:50pm
Heather Hurlburt

PRESIDENT WILLIAM J. CLINTON
INTERNET WEBCAST
WASHINGTON, DC
July 7, 2000

Good morning. Earlier this week, we launched a new and improved White House web site at www.whitehouse.gov. Today I want to talk a little about that website – and about our other efforts to use technology to bring government closer to the American people .

I'm proud to have been the President who brought the White House into the digital age. When I became President, there were just 50 websites on the worldwide web. Now there are 17 million, and almost 50 million households on-line in the United States alone. It was only seven years ago that we began to use e-mail at the White House, and six years ago that we launched the very first White House web site. Our website now has more than 9,000 pages of information – and that's not counting the archives. We've redesigned and updated it, to keep pace with its growth and the rapid changes in technology.

The new and improved White House website is another important step in our efforts to make government high-speed, high-tech, and user-friendly. We're bringing information that matters into people's homes – policy papers, a citizens' handbook, links to federal agencies. We've also made it easier to find the features that visitors use most – like e-mailing the White House, taking an on-line tour, or finding special activities for kids. And we've made the website a permanent part of the Executive Office of the President, so that future Presidents will be able to change it to suit their needs as easily as they can change the furniture in the Oval Office.

Under the leadership of Vice President Gore, we have used information technology to bring government closer to citizens in many other ways. People are now using U.S. government websites to file their taxes, compare their Medicare options, and find good jobs. They're tapping into the latest health research, browsing the vast collections of the Library of Congress, and following along with NASA's missions in outer space. And we're in the process of creating a single, customer-focused website – www.firstgov.gov -- where Americans can find every on-line resource offered by the federal government.

But we must do more to ensure that the benefits of the information revolution flow to every American. That means working to close the digital divide, to put computers in every classroom, and to train our teachers to make the most of them. We must also pay attention to the issues of computer security and privacy, so that the newest technology doesn't undermine our oldest values.

Eighty-one years ago this week, Woodrow Wilson became the first President to communicate by radio. On his way home from Europe, President Wilson used the radio, after several unsuccessful efforts, to call the young Franklin Roosevelt, then Assistant Secretary of the

Navy back in Washington. It wasn't immediately clear how this new technology would be used, or that in 15 years, Roosevelt as President would be making radio broadcasts that 80 percent of the nation would hear. But it was clear that a new door to the future had opened.

We are at just such a moment again today – and the new White House website is just one small step toward bringing government more fully into the Information Age. We have barely begun to understand how information technology will change our lives. But those of us in government have a responsibility to use these new tools to expand the reach of democracy and give more people a chance to live out their dreams.

I'll see you online at whitehouse.gov. And thanks for logging on.

# # #

So, anyway, we've come a long way. And I'd like to give you some sense of history about this, because interestingly enough, this gathering at the White House, which I think is truly historic, is in a line of such developments in this house that has shaped our country's history of communications and networking. One hundred and thirty-nine years ago, here at the White House, America celebrated our first technological revolution here in communications. That was the year Queen Victoria sent the very first transatlantic **telegraph** transmission to President Buchanan, right here. And later, the first telephone in Washington, DC, was located in a room upstairs, the same room in which Woodrow Wilson managed the conduct of America's involvement in World War I. So we've seen a lot of interesting technological developments over time in the White House. 1858

Now we celebrate the incredible potential of the Internet and the World Wide Web. When I first became President, which wasn't so long ago, only physicists were using the World Wide Web. Today, as Lou said, there are about 50 million people in 150 countries connected to the information superhighway. There will be 5 times as many by the year 2000, perhaps more, doing everything conceivable. We cannot imagine exactly what the 21st century will look like, but we know that its science and technology and its unprecedented fusions of cultures and economies will be shaped in large measure by the Internet.

We are very fortunate to have with us today, together for the very first time at the White House, the four individuals who gave birth to the Internet: Vincent Cerf and Bob Kahn, who were critical to the development of the Internet in the 1970's; Tim Berners-Lee, who invented the World Wide Web, which brought the Internet into our homes, offices, and schools; and David Duke, who headed the team that invented the fiber optic cable which made high-speed Internet connections possible. Their groundbreaking work has done more to shape and create the world our children will inherit than virtually any invention since the printing press. And I would like to ask all four of them to stand and be recognized now. [Applause]

The report which is being released and work that has been done is our effort to meet the challenge to make the Internet work for all of our people. Within a generation, we can make it so that every book ever written, every symphony ever composed, every movie ever made, every painting ever painted, is within reach of all of our children within seconds with the click of a mouse—which was "black eye" in the crossword puzzle yesterday. [Laughter]

Now, this potential is nothing short of revolutionary. The Vice President and I are working to connect every classroom and school library to the Internet by the year 2000 so that for the first time, all the children, without regard to their personal circumstances, economic or geographical, can have access to the same knowledge in the same time at the same level of quality. It could revolutionize education in America. And many of you are helping on that, and we are grateful.

We've also included $300 million in our new balanced budget plan to help build the next generation Internet so that leading universities and national labs can communicate in speeds 1,000 times faster than today, to develop new medical treatments, new sources of energy, new ways of working together.

But as has already been said, one of the most revolutionary uses of the Internet is in the world of commerce. Already we can buy books and clothing, obtain business advice, purchase everything from garden tools to hot sauce to high-tech communications equipment over the Internet. But we know it is just the beginning. Trade on the Internet is doubling or tripling every single year. In just a few years, it will generate hundreds of billions of dollars in goods and services.

If we establish an environment in which electronic commerce can grow and flourish, then every computer will be a window open to every business, large and small, every [p.1005] where in the world. Not only will industry leaders such as IBM be able to tap in to new markets, but the smallest start-up company will have an unlimited network of sales and distribution at its fingertips. It will literally be possible to start a company tomorrow and next week do business in Japan and Germany and Chile, all without leaving your home, something that used to take years and years and years to do. In this way, the Internet can be and should be a truly empowering force for large- and small-business people alike.

But today, we know electronic commerce carries also a number of significant risks that could block the extraordinary growth and progress from taking place. There are almost no international agreements or understanding about electronic commerce. Many of the most basic consumer and copyright protections are missing from cyberspace. In many ways, electronic commerce is like the Wild West of the global economy. Our task is to make sure that it's safe and stable terrain for those who wish to trade on it. And we must do so by working with other nations now, while electronic commerce is still in its infancy.

To meet this challenge, I'm pleased to announce the release of our new framework for global electronic commerce, a report that lays out principles we will advocate as we seek to establish basic rules for international electronic commerce with minimal regulations and no new discriminatory taxes. Because the Internet has such explosive potential for prosperity, it should be a global free-trade zone. It should be a place where Government makes every effort first, as the Vice President said, not to stand in the way, to do no harm.

We want to encourage the private sector to regulate itself as much as possible. We want to encourage all nations to refrain from imposing discriminatory taxes, tariffs, unnecessary regulations, cumbersome bureaucracies on electronic commerce.

Where Government involvement is necessary, its aim should be to support a predictable, consistent, legal environment for trade and commerce to flourish on fair and understandable terms. And we should do our best to revise any existing laws or rules that could inhibit electronic commerce. We want to put these principles into practice by January 1st of the year 2000.

Today I am taking three specific actions toward that goal and asking the Vice President to oversee our progress in meeting it.

First, I'm directing all Federal department and agency heads to review their policies that affect global electronic commerce and to make sure that they are consistent with the five core principles of this report.

Second, I'm directing members of my Cabinet to work to achieve some of our key objectives within the next year. I'm directing the Treasury Secretary, Bob Rubin, to negotiate agreements where necessary to prevent new discriminatory taxes on electronic commerce. I'm directing our Ambassador of Trade, Charlene Barshefsky, to work within the WTO, the World Trade Organization, to turn the Internet into a free-trade zone within the next 12 months, building on the progress of our landmark information technology agreement and our global telecommunications agreement, which eliminated tariffs and reduced trade barriers on more than one trillion dollars in products and services. I'm directing Commerce Secretary Daley to work to establish basic consumer and copyright protections for the Internet, to help to create the predictable legal environment for electronic commerce that we need and to coordinate our outreach to the private sector on a strategy to achieve this. I'm also directing the relevant agencies to work with Congress, industry, and law enforcement to make sure Americans can conduct their affairs in a secure electronic environment that will maintain their full trust and confidence. Next week, Secretary Daley and Ira Magaziner will lead a delegation to Europe to present our vision for electronic commerce to our European trading partners.

Third, I call on the private sector to help us meet one of the greatest challenges of electronic commerce, ensuring that we develop effective methods of protecting the privacy of every American, especially children who use the Internet. Many of you have already begun working with Chairman Pitofsky and Commissioner Varney at the Federal Trade Commission on this issue. I urge you to continue that work and to find new ways [p.1006] to safeguard our most basic rights and liberties so that we can trade and learn and communicate in safety and security.

Finally, it is especially important, as I said last week, to give parents and teachers the tools they need to make the Internet safe for children. A hands-off approach to electronic commerce must not mean indifference when it comes to raising and protecting children. I ask the industry leaders here today to join with us in developing a solution for the Internet as powerful for the computer as the V-chip will be for television, to protect children in ways that are consistent with the first amendment.

Later this month, I will convene a meeting with industry leaders and groups representing Internet users, teachers, parents, and librarians to help parents protect their children from objectionable content in cyberspace. Today we act to ensure that international trade on the Internet remains free of new discriminatory taxes, free of tariffs, free from burdensome regulations, and safe from piracy.

In the 21st century, we can build much of our prosperity on innovations in cyberspace in ways that most of us cannot even imagine. This vision contemplates an America in which every American, consumers, small-business people, corporate CEO's, will be able to extend our trade to the farthest reaches of the planet. If we do the right things now, in the right way, we can lead our economy into an area where our innovation, our flexibility, and our creativity yield tremendous benefits for all of our people, in which we can keep opportunity alive, bring our people closer to each other, and bring America closer to the world. I feel very hopeful about this, and I assure you that we will do our part to implement the principles we advocate today.

Thank you very much.

Note: The President spoke at 3:08 p.m. in the East Room at the White House. In his remarks, he referred to Louis Gerstner, chairman and chief executive officer, IBM; and Macadara MacColl, managing director, Parent Soup.

Source: United States. Executive Office of the President, Weekly Compilation of Presidential Documents, Week Ending Friday, July 4, 1997 (Washington, D.C.: U.S. Government Printing Office, 1997), 33:1003-1006

Turn to Previous Page Turn to Next Page

Turn to Previous Page Turn to Next Page

Remarks Announcing the Electronic Commerce Initiative,
July 1, 1997

Thank you very much, Mr. Vice President. For those of you who did not know what he was talking about, we went to a Broadway show last night, and there were three guys in the show who did the Macarena in the show. So after it was over, I thought it only fair when the Vice President spoke they come up and do the Macarena while—it was sort of background music, you know. [Laughter]

Lou Gerstner, thank you for being here. That was a remarkable statement, and the Vice President gave you a remarkable introduction. I never before thought of you as a gazelle, but I always will now. [Laughter]

Thank you, Macadara MacColl, for the work you do and for the fine words you spoke. To the members of the Cabinet and the administration and people here from industry and consumer groups, I thank all of you. I especially want to thank for this remarkable report all the agencies who worked on it and, in particular Ira Magaziner, who did a brilliant job in bringing everybody together and working this out over a very long period of time. And we thank you for what you did on that. Thank you all. I thank the Members of Congress for being here, Congressmen Gejdenson, Gordon, Markey, and Flake, and for their interest in these issues.

I had two disparate experiences in the last few days that would convince a person of limited technological proficiency, like myself, that the world is changing rather dramatically. You have to remember now, the Vice President coined the term information superhighway 20 years ago, back when I didn't even have an electric typewriter. [Laughter] But anyway, I had these two experiences which were very interesting to me. It's sort of a mark of how our world is changing.

As you may have seen in the press, the oldest living member of my family, my great uncle, passed away a few days ago, and so I went back to this little town in Arkansas where I was born. And when I got there late at night, I drove out in the country for a few miles to my cousin's house where the family was gathering. And she has a son who is in his mid-thirties now who lives in another small town in Arkansas, who, after we talked for 5 minutes, proceeded to tell me that he played golf on the Internet several times a month from his small town in Arkansas with an elderly man in Australia who unfailingly beat him. [Laughter] An unheard of experience just a few years ago. He knows this guy. He's explaining to me how he finds this man.

Then he says, "My brother likes to play backgammon on the Internet, and it got so I couldn't talk to him. But now I know how I can go get him out of his game, and he can go find a place to come have a visit with me, and they can hold the game while we have an emergency talk." I mean, these whole conversations, the way people—it was just totally unthinkable a few years ago.

And then Sunday, the New York Times crossword puzzle—I don't know if you saw it, but it was for people like me. It was entitled "Technophobes." [Laughter] And I'm really trying to overcome my limitations. I'm technologically challenged, and I'm learning how to do all kinds of things on the computer because Chelsea is going off to school, and I need to be more literate. But you ought [p.1004] to go back and pull this, all of you who are now into cyberspace, and see if you can work your way back to another world because they had high-tech clues with common answers. Like floppy disk was a clue; the answer was frisbee. [Laughter] Hard drive was a clue; the answer was Tiger's tee shot. [Laughter] Digital monitor was the clue; the answer was manicurist. [Laughter]

Proclamation 7164—National Consumer Protection Week, 1999,
January 29, 1999

By the President of the United States
of America
A Proclamation

Consumers are too often the target of unfair, deceptive, or fraudulent practices. Modern advances in telecommunications and marketing technology have dramatically increased both the sophistication and the potential threat of such practices. Perpetrators of fraud can reach consumers across the country through the Internet, on television, the **telephone**, or by direct mail, misrepresenting themselves as legitimate business people. Because their proposals appear legitimate, these unscrupulous operators frequently succeed in cheating vulnerable consumers out of hard-earned dollars.

One of the most damaging fraudulent practices is credit fraud. Credit fraud—stealing credit cards or credit identities and cheating consumers through deceptive or abusive lending practices—can be difficult to recognize. Fraudulent credit transactions are often complicated and can occur when perpetrators hide or fail to disclose essential information to consumers. By stealing consumers' credit identities, criminals can run up huge debts and ruin their victims' credit records. And credit fraud costs all of us in higher interest rates and fees.

The best defense we have against credit fraud is education. The Federal Trade Commission (FTC), the National Association of Consumer Agency Administrators, the U.S. Postal Inspection Service, the American Association of Retired Persons, the National Consumers League, the Consumer Federation of America, and the National Association of Attorneys General are working in partnership to inform Americans about the dangers of credit fraud. As part of this effort, the FTC and its partners offer information on-line, by **telephone**, and in writing to alert consumers about the warning signs of credit fraud and how to protect themselves against it. The FTC, in cooperation with State Attorneys General and the Internal Revenue Service, is also actively prosecuting credit fraud cases that target some of our most vulnerable citizens.

I encourage all Americans to learn more about credit fraud, to read their credit reports carefully, to protect such personal information as their bank account, credit card, and Social Security numbers, and to know how to recognize the characteristics of fraudulent proposals. By using credit wisely and remaining alert to the possibility of credit fraud, we can better protect the well-being of our families and preserve our financial health and security.

Now, Therefore, I, William J. Clinton, President of the United States of America, by virtue of the authority vested in me by the Constitution and the laws of the United States, do hereby proclaim January 31 through February 6, 1999, as National Consumer Protection Week. I call upon government officials, industry leaders, consumer advocates, and the American people to participate in programs that foster credit literacy and raise public awareness about the dangers of credit fraud and other deceptive and fraudulent practices.

In Witness Whereof, I have hereunto set my hand this twenty-ninth day of January, [p.152] in the year of our Lord nineteen hundred and ninety-nine, and of the Independence of the United States of America the two hundred and twenty-third.

William J. Clinton

UNITED STATES POSTAL SERVICE

usps.com

HOUSEHOLD BUSINESS

History of the U.S. Postal Service

1775-1993

United States Postal Systems

On July 26, 1775, members of the Second Continental Congress, meeting in Philadelphia, agreed ". . . that a Postmaster General be appointed for the United States, who shall hold his office at Philadelphia, and shall be allowed a salary of 1,000 dollars per annum . . . ."

That simple statement signaled the birth of the Post Office Department, the predecessor of the United States Postal Service and the second oldest department or agency of the present United States of America.

Click Here to Return to the Table of Contents

Colonial Times

In early colonial times, correspondents depended on friends, merchants, and Native Americans to carry messages between the colonies. However, most correspondence ran between the colonists and England, their mother country. It was largely to handle this mail that, in 1639, the first official notice of a postal service in the colonies appeared. The General Court of Massachusetts designated Richard Fairbanks' tavern in Boston as the official repository of mail brought from or sent overseas, in line with the practice in England and other nations to use coffee houses and taverns as mail drops.

Local authorities operated post routes within the colonies. Then, in 1673, Governor Francis Lovelace of New York set up a monthly post between New York and Boston. The service was of short duration, but the post rider's trail became known as the Old Boston Post Road, part of today's U.S. Route 1.

William Penn established Pennsylvania's first post office in 1683. In the South, private messengers, usually slaves, connected the huge plantations; a hogs head of tobacco was the penalty for failing to relay mail to the next plantation.

Central postal organization came to the colonies only after 1691 when Thomas Neale received a 21-year grant from the British Crown for a North American postal service. Neale never visited America. Instead, he appointed Governor Andrew Hamilton of New Jersey as his Deputy Postmaster General. Neale's franchise cost him only 80 cents a year but was no bargain; he died heavily in debt, in 1699, after assigning his interests in America to Andrew Hamilton and another Englishman, R.

JOSHUA GOTBAUM
07/11/2000 01:29:10 PM

Record Type: Non-Record

To: Joshua S. Gottheimer/WHO/EOP@EOP

cc: Peter P. Swire/OMB/EOP@EOP, Glenn R. Schlarman/OMB/EOP@EOP, Richard A. Clarke/NSC/EOP@EOP, Jeffrey A. Hunker/NSC/EOP@EOP

Subject: Suggestion that Podesta Describe Critical Infrastructure Funding Issues in Wiretap Remarks

Additionally, we've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And we've taken steps to ensure that the appropriate cyber security measures are included as part of all government computer systems. Unfortunately, Congress has **thus far denied** funding for some important additional steps requested by the President, such as an internal expert review team **or an intrusion detection system for the non-defense agencies or programs to attract computer security experts to Federal service.**

---------------------- Forwarded by Joshua Gotbaum/OMB/EOP on 07/11/2000 01:27 PM ---------------------------

JOSHUA

As we discussed, what about a paragraph noting that the Congress hasn't always funded our cyber-security requests? Both Sylvia and I think it should be considered by John.

Peter P. Swire

Peter P. Swire
07/11/2000 10:19:55 AM

Record Type: Record

To: See the distribution list at the bottom of this message

cc: Lauren B. Steinfeld/OMB/EOP@EOP, Stephen J. Fuzesi/OMB/EOP@EOP, Maria Pope/OMB/EOP@EOP, Charlotte Knepper/NSC/EOP@EOP

Subject: DRAFT--Podesta Wiretap Remarks. Comments pls to Gottheimer 62554.

Attached is the first draft back from the speechwriter for John Podesta's speech at the National Press Club on Friday on wiretapping and updating law enforcement authorities for the Internet age.

The speech will likely include a longer discussion of encryption, if the clearance process on encryption has a deliverable policy in time for Friday. The current likely position seems to be to match the recent E.U. announcement, so that there would be a "free trade" zone for encryption products for the E.U. plus 8 countries, with: (1) no continued distinction between government and non-government users; (2) no continued distinction between retail and non-retail products; and (3) an ability to ship immediately rather than after a 30 day delay.

We are working on a fact sheet/press paper to accompany the speech.

Also attached is the legislative package that just went into inter-agency clearance this morning. The package reflects considerable discussion in the inter-agency working group over the past several months, as well as John's guidance on what elements from that larger proposal should be in the Administration bill. The plan is to get comments by this Thursday, but not to expect transmittal until sometime next week.

doj-cybersecurity.wp

---------------------- Forwarded by Peter P. Swire/OMB/EOP on 07/11/2000 10:02 AM ---------------------------

Joshua S. Gottheimer
07/11/2000 09:37:38 AM

Record Type: Record

To: See the distribution list at the bottom of this message

cc:
Subject: DRAFT--Podesta Wiretap Remarks. Comments pls to Gottheimer 62554.

pod-wiretap2.do

Message Sent To:

Rachael F. Goldfarb/WHO/EOP@EOP
John Podesta/WHO/EOP@EOP
Michele Ballantyne/WHO/EOP@EOP
Fern Mechlowitz/WHO/EOP@EOP
Karen Tramontano/WHO/EOP@EOP
Peter P. Swire/OMB/EOP@EOP
Joel Johnson/WHO/EOP@EOP
Thomas L. Freedman/WHO/EOP@EOP

Message Sent To:

Sally Katzen/OMB/EOP@EOP
Martin L. Yeung/OMB/EOP@EOP
Joshua Gotbaum/OMB/EOP@EOP
Victoria A. Wachino/OMB/EOP@EOP
John Spotila/OMB/EOP@EOP
Mary M. Chuckerel/OMB/EOP@EOP
Daniel J. Chenok/OMB/EOP@EOP
Glenn R. Schlarman/OMB/EOP@EOP
David W. Beier/OVP/EOP@EOP
Andrew F. Schneider/OVP/EOP@EOP

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he broke down geographic barriers that had long kept us apart, opening up a world of possibility that was never even imagined just a few years before.

Morse's invention set in a motion a technological revolution that would forever change the way man would communicate. Only a few years later, in 1858, Queen Victoria bridged the waters of the Atlantic, when she sent the first transatlantic telegraph to President Buchanan in the White House. Just two decades later, using a funnel, a cup of acid, and some copper wire, Alexander Graham Bell invented a device to give a person's voice -- not just his words – a way to travel.

Today, the great revolution in science and technology continues. Just last month, we announced a major breakthrough in science – the completed map of the entire human genome. With this map in hand, we could one day eradicate many of the most deadly diseases known to man. That map wouldn't have been possible without the computers and shared information over the Internet. From small towns to big cities, the Internet is brining millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented just thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with same access to a reservoir of information – from Shakespeare's first sonnet to the remarkable photos just taken of Mars.

This new potential also brings new risks. Because we are so interconnected, more people now have easier access to our most personal information – from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But with this opportunity comes new challenges to our most fundamental values – and the need for new laws and new protections to maintain them. Over the last seven and a half years, our Administration has taken steps to keep our laws and policies in line with the latest advances in technology. To combat cyber-terrorism, we've introduced new legislation, coordinated public-private partnerships, and increased law enforcement efforts. We've also taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. As Supreme Court William Taft once said, "Time works changes … [it] brings into existence new conditions and purposes."

Today I want to talk to you about another step we should take to keep our laws consistent with the latest advances – the updating and harmonization of existing wire tapping laws. The fundamental debate over these laws is rooted in the Fourth Amendment of the Constitution, which states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." In 1787, a person's most important "papers and effects" -- like diaries and letters -- were almost undoubtedly in their home or place of business. Our "papers and effects" were thus protected by the requirement of a warrant before the state could enter and search. But with advances in technology, people no longer relied solely on paper and pen to communicate with one another. By the turn of the 20th Century, people were using the telephone for personal calls and business transactions. [And today they're relying on the Internet.] Over the years, this has forced a debate in Congress and in the Courts over the application of the Fourth Amendment. In the 1928 Olmstead case, the Supreme Court found that conversations over the telephone were not protected by the Fourth Amendment, and therefore wiretapped conversation could submitted as evidence. Judge Brandeis disagreed and argued that, "There is, in essence, no difference between the sealed the letter and private telephone message." The 1968 Court agreed with Brandeis, when it ruled in *Katz vs. the United States* that an individual's phone conversation was protected by the Fourth Admendment, and therefore inadmissable in court proceedings. The Katz precedent is still

The court overruled because the began utilizing the telephone As With the invention fthat These laws were first debated before the Supreme Court, soon after the invention of the telephone in the 1928 *Olmstead* case. In their opinion, the Court ruled that there was no assumption of privacy over a telephone line. when the majority of the Court

While the debate over these laws dates back to the early part of the 20th Century, the fundamental question is rooted in the Constitution. The debate over these laws is rooted are laws that have been debate over these laws is rooted in the constitution.

At the heart of the debate/ question is 4th amendment laws is the 4th Amendment of history

One of the greatest challenges of any era of progress is to strike a balance between protecting privacy and civil liberties – while, simultaneously, ensuring that government and law enforcement have the tools they need to safeguard that privacy. That's a challenge that our forefathers grappled with when they wrote the Constitution, and one that our government and courts have struggled with ever since.

But circumstances require us to rise to the challenge of each new era. a And the real challenge is achieve that equilibrium without standing in the way of progress. At the heart of this issue stand the 4th AmendemThe balance -- 4th amendment ... today I'm here to talk to you about a step that crucial in that balance – wiretapping issue. That's a law that needs to be updated. Go by different cases.

to keep our laws and our government in synch with our progress

In the right hands, the computer has become an indispensible tool for education, personal and commercial business, research and development. But in criminal hands, the same computer becomes a tool of destruction.. Advances in technology also gives new tools to criminals and terrorists to get info and spread it and ...

Technology is opening up a new world of possibility, but it is also challenging our privacy in ways we might never have imagined just a few years ago. That is why, over the last seven and a half years, our Administration has taken steps to protect the privacy of all Americans: We challenged the Internet industry to work with us to raise privacy standards, including steps to protect the privacy of children on-line. President Clinton proposed the first set of national standards to protect the privacy of on-line medical records. And the President proposed legislation to protect the privacy of Americans' financial records.

Today I want to talk to you about

– and a host of new challenges and new questions. And in many cases, they for new laws and for new protections, and to the laws we live by. Privacy and balance

Most importantly, he set in a motion a technological revolution that would lead to first

Technology is changing so rapidly – key is Great potential/ progress/ discovery also brings great responsibility, new challenges. Just last week discovered human genome – [see genome speech]. That's something that our country and our courts have responded to since our founding, and it's something we will continue to do as we evolve as a nation. Over the last 7 years, w/ the advances medicine and technology, we've done x, y, z.

Our admin has worked hard to keep up w/ our progress (in may … ea michigan commencement, medical privacy, signed eo …) … as judge brandeis said, " update our laws"

We know that we have to make cyberspace open and free. We have to make, at the same time, computer networks more secure and resilient, and we have to do more to protect privacy and civil liberties.

One area that's always been at the forefront of concern has been privacy (4th amendment privacy principles). Particularly true w/ laws that directly relate to our civil liberties – law enforcement (balance), and wire tapping. Historically been a 4th amendment issue, which states X. key has always been balance: between public good and civil liberties.

In updating enduring constitutional values for the computer age, we need to assure that our citizens' personal data and communications are appropriately protected.

We recognize that information technology is changing rapidly and constantly providing both new security capabilities and challenges. We will never reach a "perfect solution."

Original intent of forefathers

Here of course technology is always changing.

In the 18XX… the threshold for invasion privacy – protection privacy, home, diary … assume whether or not in a sphere of privacy.

Over time it has been updated:
In 1920, when first seminal case on tapping heard – olmstead. At that time, only

In 1968, … time of the case … law changed. Katz said x … Focused on phone, although there were websites at the time. Title III out of that. Email.

In 1986, … something I worked on closely … cell phones … passed x law to keep up w/ nascent web … ECPA. Forward looking at the time.
That law says:

But now – times have indeed changed again. We need to change w/ them, like our forefather did, and at other seminal moments in our history. Since 1986, x websites have been created. More than 2.2M cable modem subscribers. Then there were only 50… now over 50M. But the law still says x. It's easier today for fed officials to gain access to my grandmother's cookie recipe she sent me on aol, than a terrorists master mind plan sent on his cable modem. Cable law from 1984 says 10 days. Don't need x, y, …

Law enfrocment may obtain the legal authority to access a suspects' communications or dta
We need to update our law – harmonize them. So that equal laws for electronic tapping as wire tapping. so we can strike that balance – where cable not too difficult. Email not so easy. Privacy vs. law enforcement – so if drug, child porn.

We should update our laws so they do: x, y, z

Conclusion

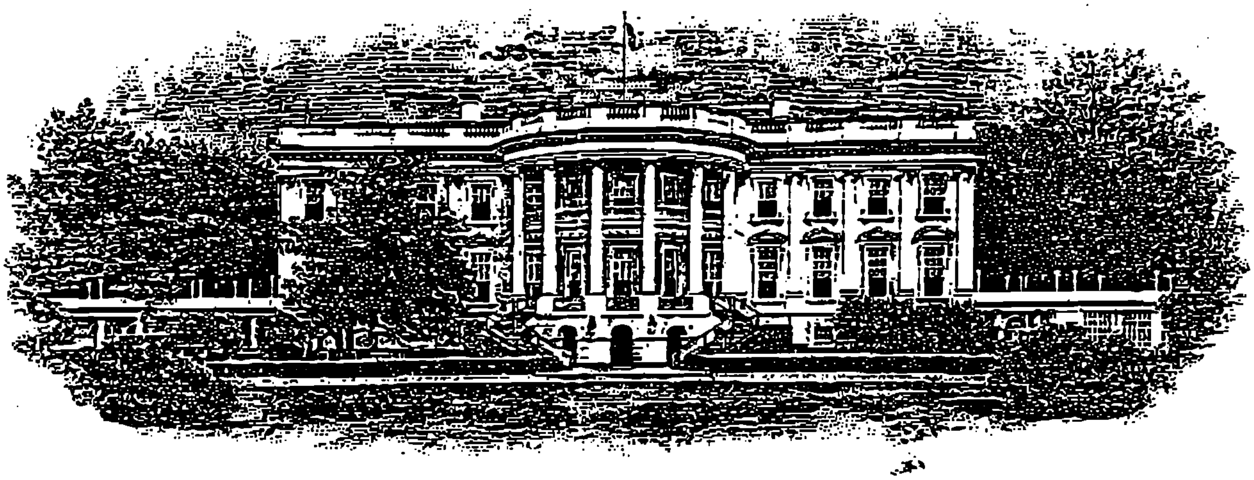
In the early years of our republic, Thomas Jefferson said, "America's institutions must move forward hand-in-hand with the progress of the human mind." Today, the progress of the human mind is certainly racing forward at break-neck speech. We must work together to ensure that our democracy/ and our laws keep pace. "

THE WHITE HOUSE

WASHINGTON

EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE OF THE CHIEF OF STAFF



Please Deliver To: Josh

Fax Number: 62505

Sender: Todd Plants

Date: 11 July 2000

Pages Including Cover: 7

Message: NIAF Speech - 6 June 2000

NOTE: **The information contained in this facsimile message is CONFIDENTIAL and intended for the recipient ONLY. If there is any problem with this transmission or you mistakenly received this facsimile, please call (202) 456-6798. Thank You.**

CHIEF OF STAFF JOHN D. PODESTA
REMARKS FOR NATIONAL ITALIAN AMERICAN FOUNDATION
ROME, ITALY
As Delivered
June 6, 2000

Ack: NIAF President Joe Cerrell; Mayor Rutelli; Elisa Gabrella Wilson; Justice Scalia; Ambassador Foglietta; Frank Guarini; Joe DelRasso.

Thank you for that kind introduction. On several occasions I've had the opportunity to address gatherings of the National Italian American Foundation. Whether in Washington DC or Rome, I always feel right at home.

It obviously wasn't a tough sell to get me over here. Of course, I wanted to see all of you ... tour Rome in its millennial splendor, and bask in the Italian sun. But, to be honest, this trip was really an excuse to spend a few waking hours with my wife, Mary Podesta, who you'll get to hear from later.

It's always nice to have an opportunity to get back to your roots. My grandfather, Antonio Podesta, was born in Né, a small town near Genoa. He labored in the shipyards of Genoa, until he moved to America in the late 1890s. It was near Genoa where my grandmother, Francesca, perfected her pesto, cima, and ravioli. And where my grandparents learned the importance of family and of community, the benefits of tradition and culture, and the meaning of hard work.

These are values that were passed on to me, and to many Italians, in cities across the globe – from the Northwest Side of Chicago... to right here in Rome. They are the values that organizations like NIAF were built on and that many of us hope to pass on to our children. They have not only led to Italy's progress, but have contributed to its role as a world leader and innovator.

Time and again Italy has been out in front. During the 15th Century, in the face of doubts and danger, the Italian explorer Christopher Columbus set sail across vast oceans for the riches of the New World. Even then, international trade played a fundamental role in Italy's economy. Two centuries later, the Italian astronomer and inventor, Galileo Galilei, advanced the laws of mathematics and physics over the teachings of the church. And, in the early 20th Century, the Nobel Prize-winning physicist, Guglilelmo Marconi, defied all odds when he sent the first ever short wave wireless radio transmission.

Today, in the dawn of the 21st Century, that innovative spirit still shines brightly on Italy. But, from the coast of Genoa... to the lagoon of Venice, from the mountains of the Alps to the hills of Sicily, both the pace of that progress and the nature of those challenges *have* changed. Modern advances in science and technology have erased borders, bringing people from all nations closer together, forming an interconnected, global community. This afternoon, I want to talk to you about the opportunities, impact, and responsibilities that come with this change – not just here in Italy, but all over the world. I can't compete with Mario Gabelli and the last panel on tips to make money, but I do hope I can add a few thoughts about how we build not only a new economy, but one that respects our old values.

We are all part of this new economy, in this new world: an economy in which wealth derives not only from the ore in the ground or the might of our factories, but from the power of our minds. A world in which nations are linked through luminous ties of commerce and communications. A world in which half a million airline passengers, 1.4 billion e-mail messages, and $1.5 trillion dollars cross national borders every single day.

Globalization is tearing down barriers between nations, economies, and cultures – and building networks that link our fates together. It is revolutionizing the way we work, live, and relate to each other across national boundaries. Communications technology and the Internet are opening trade in services and ideas and transmitting knowledge to the most remote reaches of the planet.

What is at stake for us in the 21st Century is whether we can have an international economy that works for all of us – that spurs growth, lifts lives, and sustains the environment. We must forge a trading system that honors the values we hold so dear. We can neither resist economic change – nor simply tell people to fend for themselves. We must build a global economy with a human face. We need to ensure that working people everywhere feel that they have a stake in global trade, a place for decent work, and a chance at a better life. To get there, leaders from business, government and civil society are going to have to come together – and recognize that globalization and information technology have made us all interdependent.

A strong global trading system is good for all the nations of the world. It is certainly good for America, where our surging exports create millions of new jobs. The United States has 4 percent of the world's people and 22 percent of its wealth. Our cutting edge industries, from software to aerospace to biotech to motion pictures, lead the world.

But it cannot be that a few of us live on the cutting edge while too many live on the bare edge of survival. Right now, 6 billion people live on our planet. 3 billion live on less than $2 a day, 1.3 billion people survive on $1 a day or less, which the UN defines as absolute poverty. 125 million children of grammar school age don't attend school. The global community cannot survive as a tale of two cities: one modern and integrated, a cell phone in every hand and a McDonalds on every corner, the other mired in poverty and increasingly resentful of the world passing by. That's why we must work together to ensure that developing countries have the capability to take advantage of the explosion of technology and the growth of international trade.

We need a global economic system that tears down barriers of trade, builds new opportunities, invests in education and health care, spreads information technology to villages as well as villas, raises prosperity, and lifts lives in every country on every continent. That's why President Clinton worked to pass the Trade and Development Act, which will expand our access to Sub-Saharan Africa, and to the Caribbean Basin. And why we are fighting so hard to bring China into the WTO and to pass Permanent Normal Trade Relations for China. And why we are grow stronger. But the very forces that make this a time of hope also carry the portent of risk and division. We must not be so dazzled by the bright promise of technology, and the velocity of prosperity, that we lose sight of our fundamental values: to strengthen work and family at home... to foster peace, freedom, and prosperity abroad... to enhance opportunity for all people. These are values that many of us share – native Italian, or Italian-American. They have contributed to Italy's success ... they have led to America's prosperity... and they are helping to build a stronger, more interconnected world. Thank you.

Draft 07/11/00 9:30am
Gottheimer/ Swire

CHIEF OF STAFF JOHN PODESTA
REMARKS TO PRESS CLUB ON ELECTRONIC WIRETAPPING
WASHINGTON, DC
July 14, 2000

This week millions of Americans are waiting in line to buy a hotly anticipated book. No it's not Harry Potter. [*hold up book*] It's actually *Protecting Electronic Messaging* by John Podesta -- a book I wrote when I was on the Hill a few years ago. I'll be signing copies after the speech. Buy one for each of your children.

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn't even imagined just a few years before.

Morse's invention set in a motion a technological revolution that would forever change the way man would communicate. Only a few years later, in 1858, Queen Victoria bridged the waters of the Atlantic, when she sent the first transatlantic telegraph to President Buchanan in the White House. Just two decades later, using a funnel, a cup of acid, and some copper wire, Alexander Graham Bell invented a device to give voice -- not just words – a way to travel.

Today, the great revolution in communication technology continues. From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a remarkable reservoir of information – from Shakespeare's first sonnet to the remarkable photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values – and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information – from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has worked to buid a framework for trust and security in this new world of electronic networks. We recognize that it is the private sector, that must lead in implementing network and cyber secirity. We know that the governments needs to ~~taken steps to~~ keep our laws and policies in line with the latest advances in technology. Privacy and civil liberties much be strengthened by all our actions.

The framework we are building has many parts. To combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. Just this February, in his Cyber

Draft 07/11/00 5pm
Gottheimer/ Swire

CHIEF OF STAFF JOHN PODESTA
REMARKS TO NATIONAL PRESS CLUB
ON PRIVACY AND ELECTRONIC WIRETAPPING
WASHINGTON, DC
July 14, 2000

This week millions of Americans are waiting in line to buy a hotly anticipated book. No it's not Harry Potter. [*hold up book*] It's actually *Protecting Electronic Messaging* by John Podesta -- a book I wrote when I was on the Hill a few years ago. I'll be signing copies after the speech. Buy one for each of your children.

Today I want to return to some of the topics from my not-quite best-selling book – particularly the issue of how to protect privacy and civil liberties, while also protecting public safety in an electronic age. There are three prevailing themes in this discussion: The first is how to update our laws and practices in the face of changing technology. The second is how to harmonize and bring consistency to the rules for law enforcement access to our different forms of communication. Finally, is how to both protect privacy and civil liberties online, while also protecting public safety.

To understand what these themes mean today we have to go back to the history.

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn't even imagined just a few years before.

[Morse's invention set in a motion a technological revolution that would forever change the way man would communicate. Only a few years later, in 1858, Queen Victoria bridged the waters of the Atlantic, when she sent the first transatlantic telegraph to President Buchanan in the White House. Just two decades later, using a funnel, a cup of acid, and some copper wire, Alexander Graham Bell invented a device to give voice -- not just words – a way to travel.]

Today, the great revolution in communication technology continues. From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a remarkable reservoir of information – from Shakespeare's first sonnet to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values – and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information – from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages.

Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has worked to build a framework for trust and security in this new world of electronic networks. We've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And to combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. This February, in his Cyber Security Summit, the President emphasized the primary role and responsibility of the private sector in ensuring computer and network security. As you know, most computers and networks that we rely upon every day are owned and operated by the private sector. It's only right that they – not the government -- take the leading role in making security a standard part of the Internet.

The private sector is also taking a leading role in using strong encryption to guarantee the security and privacy in electronic messages. Our Administration has already moved to liberalize our export controls on encryption, allowing more companies to export the technology to more end users. And we've done so while maintaining the structure necessary to protect our national security.

Today we are taking a significant new step to update our export controls. Under new government regulations, we're taking down the barriers that prevent corporations from exporting encryption to governments and businesses in the European Union and eight other trading partners. We're also speeding up the time-to-market, by eliminating the thirty-day waiting period for exporting encryption goods.

But the private sector can't do it alone. The government also needs to protect its own systems from security risks, such as hacker attacks and computer viruses. Our Administration has already taken action to ensure that the appropriate cyber security measures are included as part of all government computer systems. For one thing, we will not authorize one dime of spending on government computer systems unless good security measures are in place. Moreover, the President has asked Congress for additional funding, to detect computer attacks, to hire and train more security experts, and to create an internal expert review team. Unfortunately, Congress is standing in the way of our efforts, by refusing to supply the critical funds needed to put these initiatives in place. If Congress is preparing for the 21st Century, they're doing it at a 19th Century pace. We think Congress should pick up the pace and provide the protections that are essential to America's cyber security.

Supreme Court Justice Louis Brandeis once said, "Time works changes … [it] brings into existence new conditions and purposes." I want to talk to you about another step we should take to build the framework of cyber security and trust: keeping our laws consistent with the latest advances by the updating of existing wiretap laws. At the heart of the issue is the Fourth Amendment, which states that, "The right of the people be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

In 1787, a person's most important "papers and effects" -- like diaries and letters -- were almost undoubtedly in their home or place of business. These papers were protected by the requirement of a warrant before the state could enter and search. But over time, with advances in technology, people no longer rely solely on paper and pen to communicate with one another. By the turn of the 20th Century, people were using the telephone for personal calls and business transactions. By the 1980s, Americans were using e-mail. Looking ahead, even more of our "papers and effects," like word processing software and files, may be kept outside of the home. These advances in technology have forced an ongoing debate in Congress and in the Courts over the application of the Fourth Amendment.

In the 1928 *Olmstead* case, the Supreme Court found that conversations over the telephone were not protected by the Fourth Amendment, and therefore wiretapped conversation could be submitted as evidence. [*Judge Brandeis disagreed and argued that, "There is, in essence, no difference between the sealed letter and private telephone message." Wiretaps of phones, Brandeis argued, invaded the privacy of people on both ends of the line – the same privacy the framers intended to protect with the Fourth Amendment.*]

The 1968 Court agreed with Brandeis, when it ruled in *Katz vs. the United States* that an individual's phone conversation was protected by the Fourth Amendment, and therefore inadmissible in court proceedings. Later that year, Congress responded to the Court's decision by passing new legislation with strict standards for all wiretaps.

Title III of the 1968 Crime Control and Safe Streets Act required a court order and high-level Justice Department approval for all phone wiretaps. It only allowed wiretaps in the most serious crimes, such as espionage, treason, and crimes of violence. And, in those cases, it required detailed annual reports on the number and nature of all taps. Most significantly, Title III ruled that any information attained outside the parameters of the law was inadmissible in court.

Title III remained relatively untouched until the 1980s, when cellular telephone service, e-mail, and other computer-to-computer communication began to put new demands on the 1968 law. Title III of the 1968 law only applied to wire and voice communications – not to wireless phone conversations or e-mail. But by 1984, there were more than 7,000 Americans using cellular phones, and more than 400,000 logging onto electronic mail.

In response, under the leadership of Senator Leahy, Congress once again updated its laws to keep pace with changing technology. Before the 1968 Electronic Communications Privacy, ECPA, the government could use an electronic wiretap to monitor an individual's e-mails with a mere subpoena. ECPA changed that, and put in place many of the protections the courts had given to phone conversations two decades earlier.

ECPA did several things: it made clear that wireless voice communications were covered to the same degree as wire voice communications. [*It extended some, but not all, privacy protections to electronic communications intercepted in real-time. It set standards for access to stored e-mail and other electronic communications, and it adopted the trap and trace statute, governing real-time "interception" of "numbers dialed on a phone line." ECPA also made it a* *federal crime to intercept electronic mail, data transmission and other electronic communications.*] This legislation was a big step, and one that was sorely needed with the advent of electronic communication.

Today, ECPA – like its predecessors – has, in many ways, become outdated by new advances in computer technology and electronic communication. Our country, and the world, is increasingly more digital … increasingly more interactive. Since the passage of ECPA, we've seen a communications revolution with the rise of the cell phone and the development and use of the World Wide Web.

Today there are more 360 million cell phone users, and more than 50 million households online in the United States. That's an increase of more than 1250% since 1984 alone. More than 1.4 billion e-mails change hands each and every day. Computer users today send e-mail from their home phone lines through Internet Service Providers, and they download files and e-mails onto shared servers at work. A growing number of Americans – 2.2 million – log on to the Internet and send e-mail through cable modems -- a means of connection that wasn't even considered when ECPA was written.

ECPA was not devised to address many of the issues related to these newer, faster means of electronic communication. It doesn't extend Title III protections to the interception of e-mail that you send to your friend or business partner. It doesn't include other essential provisions – like the scope of crimes covered ... and the need for Justice Department approval. And ECPA doesn't include a statutory suppression rule for government violations.

What does this mean? It means that data transmitted over networks is not afforded full privacy protection. It means that many of the protections in the wiretap law do not apply to email and other Internet services Americans often use. And it means that inconsistent standards apply to government access to information.

Basically, the same e-mail, if sent different ways – through cable, phone lines, or an ISP -- is subject to different privacy standards. Considering the extent to which our electronic correspondence contains our most sensitive thoughts and information -- shouldn't they count as the "papers and effects" mentioned in the Fourth Amendment? It's time to adopt legislative protections that map Fourth Amendment principles onto the latest technology. It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations.

Today I would like to discuss several legislative proposals that would make this happen. Congress is already considering some of those proposals, and we believe that we can work with them to get them done this year.

First, some current statutes apply to criminals who use hardware "devices" but not to those who commit identical crimes using software instead. Such telephone-era laws should be clearly updated to apply to the Internet era where hardware and software are interchangeable. One of our Administration's central principles has been *technology neutrality* -- the idea that the government and the laws should be generally neutral between different technologies. In our proposed legislation, we would amend statutes that are hardware-specific or use 'devices" and other outmoded language. We would also continue to study whether any additional legislative responses are appropriate to distributed denial-of-service or other new threats.

Second, we need to achieve parity in the way the laws apply to different forms of communication. As I mentioned, the current law sets stricter standards for law enforcement access to "wire" communications such as telephone calls than for "electronic" communications such as e-mail. The market should play the central role in picking technological winners and losers, not Congress or the regulators.

In order to achieve this neutrality, we propose to harmonize the legal standards that apply to law enforcement access to e-mails, telephone calls, and cable services. For more than 30 years, federal law has set a tough, but manageable standard for when law enforcement officers can listen to the contents of phone calls. Today, the same legal protections should apply equally to electronic communication and to telephone communication. *[These protections include: the need for high-level approval within the Department of Justice; authorize use for only the most serious crimes, and the suppression of evidence in court if the rules are not followed.]*

At the same time, we propose to change the standards that apply to cable services. Under the current Cable Act, even where there is clear proof of serious crimes, law enforcement officials cannot gain access to subscriber records, unless the customer first can contest the issue in court. With our proposal, we would retain the underlying purpose of the Cable Act to keep confidential the list of shows that a customer has watched. But, when cable systems are used to access the Internet, we believe the rules should be the tough but manageable standards we also support for e-mails and telephone calls.

Third, we need to seek *balance* among crucial goals -- including the protection of public safety, the achievement of economic growth and digital opportunity, and the preservation of privacy and civil liberties. That's a challenge that our forefathers grappled with when they wrote the Constitution, and one that our government and courts have struggled with ever since. Our aim should be to enhance law enforcement authorities ability to address unlawful conduct, but also to enhance privacy and civil liberties on the Internet.

For example, we need to update the longstanding legal rules that govern when law enforcement can track the identity of those with whom we communicate. Our "trap and trace" rules come from the era of the traditional telephone network, when one company offered nationwide phone service. *[Telephone service today is offered by a wide variety of companies that offer local, long distance, and wireless services. Tracing a phone call often requires separate subpoenas in the various courts where each of the companies operates. The problem in tracing Internet communications to their source can be even worse. The structure of the Internet means that communications are routinely shuttled among many nodes, often in different federal court districts.]*

Today, we are proposing ways to make these "trap and trace" rules more effective for law enforcement, while also assuring privacy and civil liberties. We believe that a federal court should be able to issue one order to trace a communication to its source, and that order should be effective nationwide. We also believe that there should be greater judicial oversight of trap and trace authorities. Federal law should make clear that such orders should only be issued after a judicial officer has determined that the proper factual showing has been made.

[*These are all steps that we can take this year to update and harmonize our laws so that they protect privacy and civil liberties online, and protect the public safety.*]

In the early years of our republic, Thomas Jefferson said, "America's institutions must move forward hand-in-hand with the progress of the human mind." Today, the progress of the human mind is certainly racing forward at an extraordinary pace. Technology is opening up a new world of possibility -- but it is also challenging our privacy in ways we might never have imagined. As in any era of great progress, we must work together to ensure that our democracy and our laws keep pace with our technology -- and that we protect our civil liberties, not just the law enforcement mechanisms that were instituted to preserve them.

Thank you.

Draft 07/11/00 5pm
Gottheimer/ Swire

CHIEF OF STAFF JOHN PODESTA
REMARKS TO NATIONAL PRESS CLUB
ON PRIVACY AND ELECTRONIC WIRETAPPING
WASHINGTON, DC
July 14, 2000

This week millions of Americans are waiting in line to buy a hotly anticipated book. No it's not Harry Potter. [*hold up book*] It's actually *Protecting Electronic Messaging* by John Podesta -- a book I wrote when I was on the Hill a few years ago. I'll be signing copies after the speech. Buy one for each of your children.

Today I want to return to some of the topics from my not-quite best-selling book – particularly the issue of how to protect privacy and civil liberties, while also protecting public safety in an electronic age. There are three prevailing themes in this discussion: The first is how to update our laws and practices in the face of changing technology. The second is how to harmonize and bring consistency to the rules for law enforcement access to our different forms of communication. Finally, is how to both protect privacy and civil liberties online, while also protecting public safety.

To understand what these themes mean today we have to go back to the history.

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn't even imagined just a few years before.

[Morse's invention set in a motion a technological revolution that would forever change the way man would communicate. Only a few years later, in 1858, Queen Victoria bridged the waters of the Atlantic, when she sent the first transatlantic telegraph to President Buchanan in the White House. Just two decades later, using a funnel, a cup of acid, and some copper wire, Alexander Graham Bell invented a device to give voice -- not just words – a way to travel.]

Today, the great revolution in communication technology continues. From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a remarkable reservoir of information – from Shakespeare's first sonnet to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values – and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information – from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages.

Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has worked to build a framework for trust and security in this new world of electronic networks. We've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And to combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. This February, in his Cyber Security Summit, the President emphasized the primary role and responsibility of the private sector in ensuring computer and network security. As you know, most computers and networks that we rely upon every day are owned and operated by the private sector. It's only right that they – not the government -- take the leading role in making security a standard part of the Internet.

The private sector is also taking a leading role in using strong encryption to guarantee the security and privacy in electronic messages. Our Administration has already moved to liberalize our export controls on encryption, allowing more companies to export the technology to more end users. And we've done so while maintaining the structure necessary to protect our national security.

Today we are taking a significant new step to update our export controls. Under new government regulations, we're taking down the barriers that prevent corporations from exporting encryption to governments and businesses in the European Union and eight other trading partners. We're also speeding up the time-to-market, by eliminating the thirty-day waiting period for exporting encryption goods.

But the private sector can't do it alone. The government also needs to protect its own systems from security risks, such as hacker attacks and computer viruses. Our Administration has already taken action to ensure that the appropriate cyber security measures are included as part of all government computer systems. For one thing, we will not authorize one dime of spending on government computer systems unless good security measures are in place. Moreover, the President has asked Congress for additional funding, to detect computer attacks, to hire and train more security experts, and to create an internal expert review team. Unfortunately, Congress is standing in the way of our efforts, by refusing to supply the critical funds needed to put these initiatives in place. If Congress is preparing for the 21st Century, they're doing it at a 19th Century pace. We think Congress should pick up the pace and provide the protections that are essential to America's cyber security.

Supreme Court Justice Louis Brandeis once said, "Time works changes … [it] brings into existence new conditions and purposes." I want to talk to you about another step we should take to build the framework of cyber security and trust: keeping our laws consistent with the latest advances by the updating of existing wiretap laws. At the heart of the issue is the Fourth Amendment, which states that, "The right of the people be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

In 1787, a person's most important "papers and effects" -- like diaries and letters -- were almost undoubtedly in their home or place of business. These papers were protected by the requirement of a warrant before the state could enter and search. But over time, with advances in technology, people no longer rely solely on paper and pen to communicate with one another. By the turn of the 20th Century, people were using the telephone for personal calls and business transactions. By the 1980s, Americans were using e-mail. Looking ahead, even more of our "papers and effects," like word processing software and files, may be kept outside of the home. These advances in technology have forced an ongoing debate in Congress and in the Courts over the application of the Fourth Amendment.

In the 1928 *Olmstead* case, the Supreme Court found that conversations over the telephone were not protected by the Fourth Amendment, and therefore wiretapped conversation could be submitted as evidence. [*Judge Brandeis disagreed and argued that, "There is, in essence, no difference between the sealed letter and private telephone message." Wiretaps of phones, Brandeis argued, invaded the privacy of people on both ends of the line – the same privacy the framers intended to protect with the Fourth Amendment.*]

The 1968 Court agreed with Brandeis, when it ruled in *Katz vs. the United States* that an individual's phone conversation was protected by the Fourth Amendment, and therefore inadmissible in court proceedings. Later that year, Congress responded to the Court's decision by passing new legislation with strict standards for all wiretaps.

Title III of the 1968 Crime Control and Safe Streets Act required a court order and high-level Justice Department approval for all phone wiretaps. It only allowed wiretaps in the most serious crimes, such as espionage, treason, and crimes of violence. And, in those cases, it required detailed annual reports on the number and nature of all taps. Most significantly, Title III ruled that any information attained outside the parameters of the law was inadmissible in court.

Title III remained relatively untouched until the 1980s, when cellular telephone service, e-mail, and other computer-to-computer communication began to put new demands on the 1968 law. Title III of the 1968 law only applied to wire and voice communications – not to wireless phone conversations or e-mail. But by 1984, there were more than 7,000 Americans using cellular phones, and more than 400,000 logging onto electronic mail.

In response, under the leadership of Senator Leahy, Congress once again updated its laws to keep pace with changing technology. Before the 1968 Electronic Communications Privacy, ECPA, the government could use an electronic wiretap to monitor an individual's e-mails with a mere subpoena. ECPA changed that, and put in place many of the protections the courts had given to phone conversations two decades earlier.

ECPA did several things: it made clear that wireless voice communications were covered to the same degree as wire voice communications. [*It extended some, but not all, privacy protections to electronic communications intercepted in real-time. It set standards for access to stored e-mail and other electronic communications, and it adopted the trap and trace statute, governing real-time "interception" of "numbers dialed on a phone line." ECPA also made it a* *federal crime to intercept electronic mail, data transmission and other electronic communications.*] This legislation was a big step, and one that was sorely needed with the advent of electronic communication.

Today, ECPA – like its predecessors – has, in many ways, become outdated by new advances in computer technology and electronic communication. Our country, and the world, is increasingly more digital ... increasingly more interactive. Since the passage of ECPA, we've seen a communications revolution with the rise of the cell phone and the development and use of the World Wide Web.

Today there are more 360 million cell phone users, and more than 50 million households online in the United States. That's an increase of more than 1250% since 1984 alone. More than 1.4 billion e-mails change hands each and every day. Computer users today send e-mail from their home phone lines through Internet Service Providers, and they download files and e-mails onto shared servers at work. A growing number of Americans – 2.2 million – log on to the Internet and send e-mail through cable modems -- a means of connection that wasn't even considered when ECPA was written.

ECPA was not devised to address many of the issues related to these newer, faster means of electronic communication. It doesn't extend Title III protections to the interception of e-mail that you send to your friend or business partner. It doesn't include other essential provisions – like the scope of crimes covered ... and the need for Justice Department approval. And ECPA doesn't include a statutory suppression rule for government violations.

What does this mean? It means that data transmitted over networks is not afforded full privacy protection. It means that many of the protections in the wiretap law do not apply to email and other Internet services Americans often use. And it means that inconsistent standards apply to government access to information.

Basically, the same e-mail, if sent different ways – through cable, phone lines, or an ISP -- is subject to different privacy standards. Considering the extent to which our electronic correspondence contains our most sensitive thoughts and information -- shouldn't they count as the "papers and effects" mentioned in the Fourth Amendment? It's time to adopt legislative protections that map Fourth Amendment principles onto the latest technology. It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations.

Today I would like to discuss several legislative proposals that would make this happen. Congress is already considering some of those proposals, and we believe that we can work with them to get them done this year.

First, some current statutes apply to criminals who use hardware "devices" but not to those who commit identical crimes using software instead. Such telephone-era laws should be clearly updated to apply to the Internet era where hardware and software are interchangeable. One of our Administration's central principles has been *technology neutrality* -- the idea that the government and the laws should be generally neutral between different technologies. In our proposed legislation, we would amend statutes that are hardware-specific or use 'devices" and other outmoded language. We would also continue to study whether any additional legislative responses are appropriate to distributed denial-of-service or other new threats.

Second, we need to achieve parity in the way the laws apply to different forms of communication. As I mentioned, the current law sets stricter standards for law enforcement access to "wire" communications such as telephone calls than for "electronic" communications such as e-mail. The market should play the central role in picking technological winners and losers, not Congress or the regulators.

In order to achieve this neutrality, we propose to harmonize the legal standards that apply to law enforcement access to e-mails, telephone calls, and cable services. For more than 30 years, federal law has set a tough, but manageable standard for when law enforcement officers can listen to the contents of phone calls. Today, the same legal protections should apply equally to electronic communication and to telephone communication. *[These protections include: the need for high-level approval within the Department of Justice; authorize use for only the most serious crimes, and the suppression of evidence in court if the rules are not followed.]*

At the same time, we propose to change the standards that apply to cable services. Under the current Cable Act, even where there is clear proof of serious crimes, law enforcement officials cannot gain access to subscriber records, unless the customer first can contest the issue in court. With our proposal, we would retain the underlying purpose of the Cable Act to keep confidential the list of shows that a customer has watched. But, when cable systems are used to access the Internet, we believe the rules should be the tough but manageable standards we also support for e-mails and telephone calls.

Third, we need to seek *balance* among crucial goals -- including the protection of public safety, the achievement of economic growth and digital opportunity, and the preservation of privacy and civil liberties. That's a challenge that our forefathers grappled with when they wrote the Constitution, and one that our government and courts have struggled with ever since. Our aim should be to enhance law enforcement authorities ability to address unlawful conduct, but also to enhance privacy and civil liberties on the Internet.

For example, we need to update the longstanding legal rules that govern when law enforcement can track the identity of those with whom we communicate. Our "trap and trace" rules come from the era of the traditional telephone network, when one company offered nationwide phone service. *[Telephone service today is offered by a wide variety of companies that offer local, long distance, and wireless services. Tracing a phone call often requires separate subpoenas in the various courts where each of the companies operates. The problem in tracing Internet communications to their source can be even worse. The structure of the Internet means that communications are routinely shuttled among many nodes, often in different federal court districts.]*

Today, we are proposing ways to make these "trap and trace" rules more effective for law enforcement, while also assuring privacy and civil liberties. We believe that a federal court should be able to issue one order to trace a communication to its source, and that order should be effective nationwide. We also believe that there should be greater judicial oversight of trap and trace authorities. Federal law should make clear that such orders should only be issued after a judicial officer has determined that the proper factual showing has been made.

[*These are all steps that we can take this year to update and harmonize our laws so that they protect privacy and civil liberties online, and protect the public safety.*]

In the early years of our republic, Thomas Jefferson said, "America's institutions must move forward hand-in-hand with the progress of the human mind." Today, the progress of the human mind is certainly racing forward at an extraordinary pace. Technology is opening up a new world of possibility -- but it is also challenging our privacy in ways we might never have imagined. As in any era of great progress, we must work together to ensure that our democracy and our laws keep pace with our technology -- and that we protect our civil liberties, not just the law enforcement mechanisms that were instituted to preserve them.

Thank you.

Title III remained relatively untouched until the mid-1980s, when cellular telephone service, e-mail, and other computer-to-computer communication put new demands on the 1968 law. Title III of the 1968 law only applied to wire and voice communications – not to wireless phone conversations or e-mail. But by 1984, there were more than 7,000 Americans using cellular phones, and more than 400,000 logging onto electronic mail.

In response, under the leadership of Senator Leahy, Congress adopted the Electronic Communications Privacy Act of 1986 -- once again updating its laws to keep pace with changing technology. Before ECPA, the government could use an electronic wiretap to monitor an individual's e-mails with a mere subpoena. ECPA changed that, and put in place many of the protections the courts had given to phone conversations two decades earlier.

ECPA did several things: it made clear that wireless voice communications were covered to the same degree as wire voice communications. It extended some, but not all, privacy protections to electronic communications intercepted in real-time. It set standards for access to stored e-mail and other electronic communications, and it adopted the trap and trace statute, governing real-time "interception" of "numbers dialed on a phone line." ECPA also made it a federal crime to intercept electronic mail, data transmission and other electronic communications. This legislation was a big step, and one that was sorely needed with the advent of electronic communication.

Today, ECPA – like its predecessors – has, in many ways, become outdated by new advances in computer technology and electronic communication. Our country, and the world, is increasingly more digital ... increasingly more interactive. Since the passage of ECPA, we've seen a communications revolution with the rise of the cell phone and the development and use of the World Wide Web.

Today there are more 360 million cell phone users, and more than 50 million households online in the United States. That's an increase of more than 1250% since 1984 alone. More than over 1.4 billion e-mails change hands each and every day. Computer users today send e-mail from their home phone lines through Internet Service Providers, and they download files and e-mails onto shared servers at work. A growing number of Americans – 2.2 million – log on to the Internet and send e-mail through cable modems -- a means of connection that wasn't even considered when ECPA was written.

ECPA was not devised to address many of the issues related to these newer, faster means of electronic communication. It doesn't extend Title III protections to the interception of e-mail that you send to your friend or business partner. It doesn't include other essential provisions – like the scope of crimes covered ... and the need for Justice Department approval. And ECPA doesn't include a statutory suppression rule for government violations.

What does this mean? It means that data transmitted over networks is not afforded full privacy protection. It means that many of the protections in the wiretap law do not apply to email and other Internet services Americans often use. And it means that inconsistent standards apply to government access to information.

Basically, the same e-mail sent different ways – through cable, phone lines, or an ISP -- is subject to different privacy standards. Considering the extent to which our electronic correspondence contains our most sensitive thoughts and information -- shouldn't they count as the "papers and effects" mentioned in the Fourth Amendment? It's time to adopt legislative protections that map Fourth Amendment principles onto the latest technology. It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations.

I propose the following legislative actions:

First, some current statutes apply to criminals who use hardware "devices" but not to identical crimes that use software instead. Such telephone-era laws should be clearly updated to apply to an Internet era where hardware and software are interchangeable. One of our Administration's central principles has been *technology neutrality* -- the idea that the government and the laws should be generally neutral between different technologies. In our proposed legislation, we would amend statutes that are hardware-specific or use 'devices" and other outmoded language. We would also continue to study whether any additional legislative responses are appropriate to distributed denial-of-service or other new threats.

Second, we need to achieve parity in the way the laws apply to different forms of communication. As I mentioned, the current law sets stricter standards for law enforcement access to "wire" communications such as telephone calls than for "electronic" communications such as e-mail. The market should play the central role in picking technological winners and losers, not Congress or the regulators.

In order to achieve this neutrality, we propose to harmonize the legal standards that apply to law enforcement access to e-mails, telephone calls, and cable services. For more than 30 years, federal law has set a tough, but manageable standard for when law enforcement officers can listen to the contents of phone calls. Today, the same legal protections should apply equally to electronic communication as they do to telephone communication. These protections include: the need for high-level approval within the Department of Justice; authorize use for only the most serious crimes, and the suppression of evidence in court if the rules are not followed.

At the same time, we propose to change the standards that apply to cable services. Under the current Cable Act, even where there is clear proof of serious crimes, law enforcement officials cannot gain access to subscriber records -- unless the customer first can contest the issue in court. With our proposal, we would retain the underlying purpose of the Cable Act to keep confidential the list of shows that a customer has watched. But, when cable systems are used to access the Internet, we believe the rules should be the tough but manageable standards we also support for e-mails and telephone calls.

Third, we need to seek *balance* among crucial goals -- including the protection of public safety, the achievement of economic growth and digital opportunity, and the preservation of privacy and civil liberties. That's a challenge that our forefathers grappled with when they wrote the Constitution, and one that our government and courts have struggled with ever since. Our

Security Summit, the President emphasized the role and responsibility of the private sector in ensuring computer and network security. We've also worked to develop strong encryption tools – like those put in place by the European Union -- to provide tighter security and privacy in electronic communications.

Additionally, we've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And we've taken steps to ensure that the appropriate cyber security measures are included as part of all government computer systems. Unfortunately, Congress has not given us the necessary funding the President has requested to take additional steps, such as funding an internal expert review team.

Supreme Court Justice Louis Brandeis once said, "Time works changes … [it] brings into existence new conditions and purposes." Today I want to talk to you about another step we should take to build the framework of cyber security and trust : keeping our laws consistent with the latest advances by the updating of existing wiretap laws. At the heart of the issue is the Fourth Amendment, which states that, "The right of the people be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

In 1787, a person's most important "papers and effects" -- like diaries and letters -- were almost undoubtedly in their home or place of business. These papers were protected by the requirement of a warrant before the state could enter and search. But over time, with advances in technology, people no longer relied solely on paper and pen to communicate with one another. By the turn of the 20th Century, people were using the telephone for personal calls and business transactions. By the 1980s, Americans were using e-mail. These advances in technology have forced an ongoing debate in Congress and in the Courts over the application of the Fourth Amendment.

In the 1928 *Olmstead* case, the Supreme Court found that conversations over the telephone were not protected by the Fourth Amendment, and therefore wiretapped conversation could be submitted as evidence. Judge Brandeis disagreed and argued that, "There is, in essence, no difference between the sealed letter and private telephone message." Wiretaps of phones, Brandeis argued, invaded the privacy of people on both ends of the line – the same privacy the framers intended to protect with the Fourth Amendment.

The 1968 Court agreed with Brandeis, when it ruled in *Katz vs. the United States* that an individual's phone conversation was protected by the Fourth Amendment, and therefore inadmissible in court proceedings. Later that year, Congress responded to the Court's decision by passing new legislation with strict standards for all wiretaps.

Title III of the 1968 Crime Control and Safe Streets Act required a court order and high-level Justice Department approval for all phone wiretaps. It only allowed wiretaps in the most serious crimes, such as espionage, treason, and crimes of violence. And, in those cases, it required detailed annual reports on the number and nature of all taps. Most significantly, Title III ruled that any information attained outside the parameters of the law was inadmissible in court.