

NOTE: I'VE PUT POSSIBLE CUTS IN BRACKETS & ITALICS.

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**

*about a hidden
world, w/ secret
powers and mysterious
laws.*

96
10
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. *laws*
can't
rule

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.*]

Anecdote
After
SOP
President
de la
to
rule

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

DA
Danger

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

BUT I WAS ONE OF THEM

2.4 million = 1/2
240,000 = 1/10
24,000 = 1/100

Solke
(Imagine that)

✓?

AND I
KNOW ITS
70404
FOR
YOU
TO
BELIEVE

7 letters
1 on Jan 1/100 of 1970

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.

NOTE: I'VE PUT POSSIBLE CUTS IN BRACKETS & ITALICS.

Draft 07/12/00 7:30pm
Gottheimer/ Swire

ml

**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 [about a hidden world with secret powers and mysterious laws]. 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. ~~Not a lot of time left to sell~~ *(or you may keep a secret.)*

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.

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.]

Speech
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 a leading role in making security a standard part of the Internet.

The private sector is also taking a leading role in developing and 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 a framework necessary to protect our national security.

Today we are announcing significant new updates to our export controls. Under our new policy, we're providing American companies with new opportunities by permitting any encryption product to be exported to an end user 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 when exporting encryption goods to these countries.

While the private sector has a key role -- the government must also play an important part. 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 without good security measures. Moreover, the President has asked Congress for additional funding in non-defense agencies, 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.~~

[STRIKE QUOTE] 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.

This debate is not a new one. In the 1928 *Olmstead* case, the Supreme Court found that warrantless wiretaps were not protected by Fourth Amendment. Louis Brandeis in his fiery dissent in defense of privacy rights 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.]

Forty years later the Court embraced Brandeis and 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.

collyer 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. That's less than 1/100 of 1 percent. [*I know it's hard to believe, but I, was, one of them.*]

actually In response, under the leadership of Senator Leahy and Congressman Kastenmeier, 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.

^{Now} 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 today ~~and growing~~ – 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. ^{re} 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.~~

we go to traditional phone calls.

Basically, the same communication, if sent different ways – through a phone call, or a dial-up modem -- 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.

Look Bush, we've had this for a year & a half ago

for a while 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.

I
~~[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.]~~

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,~~ ^Wwe 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 ^{but sensible} 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.

is not the
Harris of
make that
communication,
has been

~~challenged~~ ~~challenged~~ ~~challenged~~
prob various states / countries
court disputes

at that time the
we believe help
there should be better
judicial oversight.

2-1-09

257-
12999

8774

8774

993 97

351 / 54-0383

Adm Gen - Carni Moore has used for a report on.

Draft 07/15/00 8:45pm
Gottheimer/ Swire

ENC 3
5215
8/10/00

Under Review 371 5765

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

[Can you keep a secret?]. This week millions of Americans are waiting in line to buy a hotly anticipated book about a hidden world with secret powers and mysterious laws. No it's not Harry Potter. [hold up book.] It's actually Protecting Electronic Messaging -- a kiss and tell 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. It's common for WH officials to write this + tell books

will deliver book
see house

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.

to write book + book de en write it PEN I need to give you a little bit of history

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 motion a technological revolution that would forever change the way man would communicate.

2 enclosed
sy M
only book de ever written was PEN

In the 21st Century, 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 medical research ... to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new ~~found opportunity and~~ possibility. 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. We have to make sure the Internet is used for the benefit of people -- not to their detriment. Here why.

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 ^{on} every day are owned and operated by the private sector. It's only right that ~~they~~ – not the government -- take a leading role in making security a standard part of the Internet.

The private sector is also taking a leading role in ^{elect. netz. + comz.} ~~developing and using strong encryption~~ to ~~guarantee the security and privacy in electronic messages~~. Our Administration has already moved to liberalize export controls on encryption, allowing more companies to export the technology to more end users. And we've done so while maintaining a framework necessary to protect our national security.

Today we are announcing significant new updates to our export controls. Under our new policy, American companies can export any encryption product to an end user 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 when exporting encryption goods to these countries.

While the private sector has a key role – 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~~ cyber security measures are included as part of all government computer systems. But good security needs to be updated constantly – and it costs money. We've proposed \$90 million to help detect computer attacks, to conduct research on security technology, to hire and train more security experts, and to create an internal expert review team for ~~the~~ non-defense agencies. Unfortunately, the Congress refuses to appropriate one dime to put these initiatives in place. It's time they picked up the pace and provided the protections that are essential to America's cyber security.

Implementing strong encryption is only one step in building a framework of cyber-security and trust. We also need to keep our laws consistent with the latest advances by the updating of ^{our} existing ~~wiretap laws~~. ^{Communication Privacy} ~~Telephone laws~~ for the Internet age.] At the heart of the issue is the Fourth Amendment, which ~~states that~~ ^{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 started using the telephone for personal calls and business transactions. By the 1980s, Americans began using e-mail. Looking ahead, even more of our "papers and effects," like word processing software and files, will 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.

This debate is not a new one. In the 1928 *Olmstead* case, the Supreme Court found that warrantless wiretaps were not protected by Fourth Amendment. Louis Brandeis in his fiery dissent in defense of privacy rights 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.

Forty years later the Court embraced Brandeis and 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.

He is not a (man) (M)
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. By 1984, there were more than 7,000 Americans using cellular phones, and more than 400,000 logging onto electronic mail. ~~These conversations were not protected by Title III.~~

elect cell phone
In response, under the leadership of Senator Leahy, Congress once again updated its laws to keep pace with changing technology. ECPA, the Electronic Communications Privacy Act, put in place many of the protections the courts had given to phone conversations two decades earlier.

John
ECPA – like its predecessors – has, in many ways, become outdated by new advances in computer technology and electronic communication. Since its passage in 1986, 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 than 300 million cell phone users, and more than 50 million households online in the United States. 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 today – 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.

elect #
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.~~

call
What does this mean? It means that data transmitted over networks is not afforded the full privacy protection we give to traditional phone calls.

over current provisions to protect electronic communications
Basically, the same communication, if sent different ways – through a phone call, or a dial-up modem -- 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 Louis Brandeis foreshadowed more than seventy years ago, as the "papers and effects" mentioned in the Fourth Amendment?

no impl privacy
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 would like to discuss several legislative proposals that would make this happen. ~~These are proposals that Congress is already considering, and that I believe we can work to get done this year.~~

think for falling
proposals of MLI over
fyder. to get MLI over

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.

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 an order to trace a communication to its source -- irrespective of whether that communication has been channeled through ~~X various states/ courts.~~ ~~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. ~~That will protect our~~ ~~Here we step back~~ ~~will protect or public safety~~ ~~while~~ ~~preserving~~ ~~our~~ ~~civil~~ ~~liberties.~~

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.

Final 07/16/00 6pm

Gottheimer/ Swire

CHIEF OF STAFF JOHN PODESTA
REMARKS TO NATIONAL PRESS CLUB ON
ELECTRONIC PRIVACY
WASHINGTON, DC

~n

July 14, 2000

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

→ 147 Joke Math n -

To understand what these themes mean today we have to go back to the history.

Morse's invention set in motion a technological revolution that would forever change the way man would communicate.

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,

-- So ~~not~~ the intent is
used to ~~not~~ ~~it~~ ~~was~~ ~~intended~~
to ~~help~~ ~~people~~ ~~- etc~~
~~not~~ ~~for~~ ~~natural~~ ~~purposes~~

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 a leading role in making security a standard part of the Internet.

The private sector is also taking a leading role in developing and 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 a framework necessary to protect our national security.

Today we are announcing significant new updates to our export controls. Under our new policy, we're ~~providing~~ American companies with ~~new opportunities by permitting any~~ encryption product to be exported to an end user 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 when exporting encryption goods to these countries.

While the private sector has a key role -- 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 cyber security measures are included as part of all government computer systems. Good security costs money. We've proposed [X] millions to help detect computer attacks, to hire and train more security experts, and to create an internal expert review team for the non-defense agencies. But Congress refuses to appropriate one dime to put these initiatives in place. It's time Congress picked up the pace and provided the protections that are essential to America's cyber security.

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.

This debate is not a new one. In the 1928 *Olmstead* case, the Supreme Court found that warrantless wiretaps were not protected by Fourth Amendment. Louis Brandeis in his fiery dissent in defense of privacy rights argued that, "There is, in essence, no difference between the sealed letter and private telephone message." Wiretaps of phones, Brandeis argued, invaded the

So that he later it used to help

privacy of people on both ends of the line – the same privacy the framers intended to protect with the Fourth Amendment.

Forty years later the Court embraced Brandeis and 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.~~ By 1984, there were more than 7,000 Americans using cellular phones, and more than 400,000 logging onto electronic mail. *Text conversations were not protected by Title III*

In response, under the leadership of Senator Leahy and Congressman Kastenmeier, 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 – 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. *de Geleru... , its pass 17 1986,*

Today there are more 360 million cell phone users, and more than 50 million households online in the United States. 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 today – 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 the full privacy protection we give to traditional phone calls.

Basically, the same communication, if sent different ways -- through a phone call, or a dial-up modem -- 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 Louis Brandeis foreshadowed more than seventy years ago, 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.

Marked by [unclear]

I would like to discuss several legislative proposals that would make this happen.

Congress is already considering ~~some of these proposals~~, and I believe that we can work ~~with them~~ to get them done this year.

There are proposals that

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, ~~so that they are technology neutral.~~ ~~and use~~

Spent *proposed* *respect* *illustration* *does* *not:*

Second, we need to achieve parity in the way the laws apply to different forms of communication. 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.

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.

Retr. can I say? *our proposed legislation would [unclear] not* *15*

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 sensible standard 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

[Can you keep a secret?]. This week millions of Americans are waiting in line to buy a hotly anticipated book about a hidden world with secret powers and mysterious laws. No it's not Harry Potter. [*hold up book.*] It's actually Protecting Electronic Messaging -- a kiss and tell 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.

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 motion a technological revolution that would forever change the way man would communicate.

In the 21st Century, 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 medical research ... to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found opportunity and possibility. 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. We have to make sure the Internet is used for the benefit of people – not to their detriment.

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 a leading role in making security a standard part of the Internet.

The private sector is also taking a leading role in developing and using strong encryption to guarantee the security and privacy in electronic messages.

Our Administration has already moved to liberalize export controls on encryption, allowing more companies to export the technology to more end users. And we've done so while maintaining a framework necessary to protect our national security.

Today we are announcing significant new updates to our export controls. Under our new policy, American companies can export any encryption product to an end user 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 when exporting encryption goods to these countries.

While the private sector has a key role – 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 cyber security measures are included as part of all government computer systems. But good security needs to be updated constantly – and it costs money. [We’ve proposed \$90 million to help detect computer attacks, to conduct research on security technology, to hire and train more security experts, and to create an internal expert review team for the non-defense agencies.] Unfortunately, the Congress refuses to appropriate one dime to put these initiatives in place. It’s time they picked up the pace and provided the protections that are essential to America’s cyber security.

Implementing strong encryption is only one step in building a framework of cyber-security and trust.

We also need to keep 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 started using the telephone for personal calls and business transactions. By the 1980s, Americans began using e-mail.

Looking ahead, even more of our “papers and effects,” like word processing software and files, will 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.

This debate is not a new one. In the 1928 *Olmstead* case, the Supreme Court found that warrantless wiretaps were not protected by Fourth Amendment. Louis Brandeis in his fiery dissent in defense of privacy rights 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.

Forty years later the Court embraced Brandeis and 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.

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.

lexis.com™

[Change Client](#) [Options](#) [Feedback](#) [Sign Off](#) [Help](#)[Search](#) [Search Advisor](#) [Get a Document](#) [Check a Citation](#)[ECLIPSE™](#) [History](#)View: [KWIC](#) | [Full](#) | [Custom](#)

1 of 1

[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : [Collected Quotations](#)Terms: **brandeis** ([Edit Search](#))*1983 3,500 Good Quotes for Speakers*Copyright 1983 Gerald F. Lieberman
3,500 Good Quotes for Speakers**SUBJECT:** IMMORTALITY**LENGTH:** 18 words**SOURCE:** Louis D. **Brandeis****QUOTE:**

Men long for an afterlife in which there apparently is nothing to do but delight in heaven's wonders.

SEE-ALSO: Heaven, Hell**LANGUAGE:** ENGLISHView: [KWIC](#) | [Full](#) | [Custom](#)

1 of 1

[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : [Collected Quotations](#)Terms: **brandeis** ([Edit Search](#))

View: Full

Date/Time: Wednesday, July 5, 2000 - 6:01 PM EDT

[Search](#) | [Search Advisor](#) | [Get a Document](#) | [Check a Citation](#)
[ECLIPSE\(TM\)](#) | [History](#) | [Change Client](#) | [Options](#) | [Feedback](#) | [Sign Off](#) | [Help](#)
[About LEXIS-NEXIS](#) | [Terms and Conditions](#)

Copyright © 2000 LEXIS-NEXIS Group. All rights reserved.

lexis.com

[Change Client](#) [Options](#) [Feedback](#) [Sign Off](#) [Help](#)[Search](#) [Search Advisor](#) [Get a Document](#) [Check a Citation](#)ECLIPSE™ [History](#)View: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)[PREVIOUS](#) 5 of 18 [NEXT](#)[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : **Collected Quotations**Terms: [privacy](#) ([Edit Search](#))*Copyright 1988 Simpson's Contemporary Quotations*Copyright 1988 James B. Simpson
Simpson's Contemporary Quotations**SECTION:** The World**SUBJECT:** Law; Judicial Opinions**LENGTH:** 430 words**SOURCE:** Harry A Blackmun, Associate Justice, US Supreme Court**QUOTE:**

The states are not free, under the guise of protecting maternal health or potential life, to intimidate women into continuing pregnancies.

Majority opinion in 7-2 ruling that established the constitutional legality of abortion, 22 Jan 73

The mandated description of fetal characteristics at two-week intervals, no matter how objective, is plainly overinclusive. [It is] not medical information that is always relevant to the woman's decision, and it may serve to confuse and punish her and to heighten her anxiety.

ib

Controversy over the meaning of our nation's most majestic guarantees frequently has been turbulent. . . . Abortion raises moral and spiritual questions over which honorable persons can disagree sincerely and profoundly. But those disagreements did not then and do not now relieve us of our duty to apply the Constitution faithfully.

ib

If there is any truth to the old proverb that "one who is his own lawyer has a fool for a client," the Court . . . now bestows a *constitutional* right on one to make a fool of himself.

Dissenting opinion in 6-3 ruling that allowed a defendant to refuse counsel, 30 Jun 75

The flaw in the statute [is] that in all its applications, it operates on a fundamentally mistaken premise that high solicitation costs are an accurate measure of fraud.

Majority opinion in 5-4 ruling that struck down a Maryland statute regulating how much charities may spend on fund raising, 26 Jun 84

By placing discretion in the hands of an official to grant or deny a license, such a statute creates a threat of censorship that by its very existence chills free speech.

ib

What the Court really has refused to recognize is the fundamental interest all individuals have in controlling the nature of their intimate associations.

Dissenting opinion in 5-4 ruling that upheld the right to prohibit deviant sexual behavior, 30 Jun 86

The right of an individual to conduct intimate relationships in the intimacy of his or her own home seems to me to be the heart of the Constitution's protection of **privacy**.

lexis.com

[Change Client](#) [Options](#) [Feedback](#) [Sign Off](#) [Help](#)[Search](#) [Search Advisor](#) [Get a Document](#) [Check a Citation](#)[ECLIPSE™](#) [History](#)View: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)[PREVIOUS](#) 6 of 18 [NEXT](#)[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : **Collected Quotations**Terms: **privacy** ([Edit Search](#))*Copyright 1988 Simpson's Contemporary Quotations*Copyright 1988 James B. Simpson
Simpson's Contemporary Quotations**SECTION:** The World**SUBJECT:** Law; Judicial Opinions**LENGTH:** 330 words**SOURCE:** William O Douglas, Associate Justice, US Supreme Court**QUOTE:**

We do not sit as a superlegislature to weight the wisdom of legislation.

Majority opinion in 8-1 ruling that upheld right of states to legislate internal affairs, 3 Mar 52

We are a religious people whose institutions presuppose a Supreme Being.

Majority opinion in 6-3 ruling that allowed release of public school students for religious instruction, 28 Apr 52

The right to be let alone is indeed the beginning of all freedoms.

Dissenting opinion in 7-1 ruling that allowed radios to be played on streetcars, 26 May 52

The critical point is that the Constitution places the right of silence beyond the reach of government.

Dissenting opinion in 7-2 ruling that upheld Immunity Act of 1954, 26 Mar 56

Free speech is not to be regulated like diseased cattle and impure butter. The audience . . . that hissed yesterday may applaud today, even for the same performance.

Dissenting opinion in 5-4 ruling that banned sale of obscene books, 24 Jun 57

We deal with a right of **privacy** older than the Bill of Rights -- older than our political parties, older than our school system.

Majority opinion in 6-2 ruling that overturned state birth control laws, 7 Jun 65

Marriage is a coming together for better or for worse, hopefully enduring, and intimate to the degree of being sacred.

ib

The association promotes a way of life, not causes; a harmony in living, not political faiths; a bilateral loyalty, not commercial or social projects. Yet it is an association for as noble a purpose as any involved in any prior decisions.

ib

If discrimination based on race is constitutionally permissible when those who hold the reins can come up with "compelling" reasons to justify it, then constitutional guarantees acquire an accordionlike quality.

Dissenting opinion in 7-2 ruling that upheld discriminatory university admissions policies, 23 Apr 74

lexis.com™

[Change Client](#) [Options](#) [Feedback](#) [Sign Off](#) [Help](#)[Search ▶](#) [Search Advisor ▶](#) [Get a Document ▶](#) [Check a Citation ▶](#)[ECLIPSE™](#) [History](#)View: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)[PREVIOUS](#) 8 of 18 [NEXT](#)[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : [Collected Quotations](#)Terms: [privacy](#) ([Edit Search](#))*Copyright 1988 Simpson's Contemporary Quotations*Copyright 1988 James B. Simpson
Simpson's Contemporary Quotations**SECTION:** The World**SUBJECT:** Law; Judicial Opinions**LENGTH:** 272 words**SOURCE:** Antonin Scalia, Associate Justice, US Supreme Court**QUOTE:**

There is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the **privacy** of us all.

Majority opinion in 6-3 ruling that refused to expand police powers to search or seize evidence that they suspect may be stolen, 3 Mar 87

A search is a search, even if it happens to disclose nothing but the bottom of a turntable.

ib

We are unwilling to send police and judges into a new thicket of 4th Amendment law, to seek a creature of uncertain description that is neither a plainview inspection nor yet a "full-blown search."

ib

The Court today completes the process of converting [Title VII of the Civil Rights Act of 1964] from a guarantee that race or sex will not be the basis for employment determinations, to a guarantee that it often will.

Dissenting opinion in 6-3 ruling that employers may sometimes favor women and members of minorities over better-qualified men and whites in hiring and promoting in order to achieve better balance in their work forces, 25 Mar 87

Ever so subtly, without even alluding to the last obstacles preserved by earlier opinions that we now push out of our path, we effectively replace the goal of a discrimination-free society with the quite incompatible goal of proportionate representation by race and by sex in the workplace.

ib

A law can be both economic folly and constitutional.

Concurring opinion in 6-3 ruling that upheld state law restricting hostile takeover offers for companies incorporated within that state, 21 Apr 87

LANGUAGE: ENGLISHView: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)[PREVIOUS](#) 8 of 18 [NEXT](#)[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)

lexis.comSM

Change ClientOptionsFeedbackSign OffHelp

SearchSearch AdvisorGet a DocumentCheck a CitationECLIPSETMHistory

View: CiteKWICFullCustom

PREVIOUS9 of 18NEXT

Text OnlyDownloadFaxEmail

FOCUSTM - Narrow ResultsSave As ECLIPSEMore Like ThisMore Like Selected Text

Source: All Sources : / . . . / : Collected Quotations

Terms: privacy (Edit Search)

Copyright 1988 Simpson's Contemporary Quotations

Copyright 1988 James B. Simpson
Simpson's Contemporary Quotations

SECTION: The World

SUBJECT: Law; Judicial Opinions

LENGTH: 430 words

SOURCE: John Paul Stevens, Associate Justice, US Supreme Court

QUOTE:

When the commission finds that a pig has entered the parlor, the exercise of its regulatory power does not depend on proof that the pig is obscene.
Majority opinion in 5-4 ruling that allowed the Federal Communications Commission to prohibit the broadcasting of words that are offensive but fall short of the Court's definition of obscenity, 3 Jul 78

The 4th Amendment protects the individual's **privacy** in a variety of settings. In none is the zone of **privacy** more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home -- a zone that finds its roots in clear and specific constitutional terms: "the right of the people to be secure in their . . . houses . . . shall not be violated."

Majority opinion in 6-3 ruling that required police to have a warrant before entering a suspect's home to make an arrest, 15 Apr 80

It is not our job to apply laws that have not yet been written.
Majority opinion in 5-4 ruling that allowed consumers to use videotape recorders to tape television programs for their own use, 17 Jan 84

Although it may not be a castle, [it is the] functional equivalent of a hotel room, a vacation and retirement home or a hunting and fishing cabin.
Dissenting opinion in 6-3 ruling that upheld the search of a motor home by police without a warrant, 13 May 85

Just as the right to speak and the right to refrain from speaking are complementary components of a broader concept of individual freedom of mind, so also the individual's freedom to choose his own creed is the counterpart of his right to refrain from accepting the creed established by the majority.
Majority opinion in 6-3 ruling that an Alabama law authorizing voluntary prayer or meditation in public schools violated the 1st Amendment by encouraging religious practice, 4 Jun 85

The government must pursue a course of complete neutrality toward religion.
ib

They may not be conscripted against their will as the foot soldiers in a federal crusade.
Majority opinion in 5-3 ruling that struck down Reagan administration regulations requiring life-prolonging medical treatment for infants with severe handicaps, 9 Jun 86

lexis.com™

[Change Client](#) [Options](#) [Feedback](#) [Sign Off](#) [Help](#)[Search](#) | [Search Advisor](#) | [Get a Document](#) | [Check a Citation](#) |ECLIPSE™ [History](#)View: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)[PREVIOUS](#) 14 of 18 [NEXT](#)[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : **Collected Quotations**Terms: **privacy** ([Edit Search](#))*Copyright 1988 Simpson's Contemporary Quotations*Copyright 1988 James B. Simpson
Simpson's Contemporary Quotations**SECTION:** Humankind**SUBJECT:** Wisdom, Philosophy & Other Musings**LENGTH:** 51 words**SOURCE:** Harold Azine**QUOTE:**Happiness in the older years of life, like happiness in every year of life, is a matter of choice -- *your* choice for yourself.*The House in Webster Groves* NBC TV 16 Feb 58Happiness in old age is, more than anything else, preserving the privileges of **privacy**.
*ib***LANGUAGE:** ENGLISHView: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)[PREVIOUS](#) 14 of 18 [NEXT](#)[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : **Collected Quotations**Terms: **privacy** ([Edit Search](#))

View: Full

Date/Time: Wednesday, July 5, 2000 - 6:07 PM EDT

[Search](#) | [Search Advisor](#) | [Get a Document](#) | [Check a Citation](#)
[ECLIPSE\(TM\)](#) | [History](#) | [Change Client](#) | [Options](#) | [Feedback](#) | [Sign Off](#) | [Help](#)
[About LEXIS-NEXIS](#) | [Terms and Conditions](#)

Copyright © 2000 LEXIS-NEXIS Group. All rights reserved.

lexis.com™

[Change Client](#) [Options](#) [Feedback](#) [Sign Off](#) [Help](#)[Search](#) [Search Advisor](#) [Get a Document](#) [Check a Citation](#)ECLIPSE™ [History](#)View: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#) [PREVIOUS](#) 15 of 18 [NEXT](#) [Text Only](#) | [Download](#) | [Fax](#) | [Email](#)
[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : **Collected Quotations**Terms: **privacy** ([Edit Search](#))*Copyright 1988 Simpson's Contemporary Quotations*Copyright 1988 James B. Simpson
Simpson's Contemporary Quotations**SECTION:** Humankind**SUBJECT:** Wisdom, Philosophy & Other Musings**LENGTH:** 93 words**SOURCE:** Marshall McLuhan**QUOTE:**

The new electronic independence re-creates the world in the image of a global village.

The Gutenberg Galaxy: The Making of Typographical Man University of Toronto 62Publication is a self-invasion of **privacy**.*Counterblast* Harcourt, Brace & World 69

The more the data banks record about each one of us, the less we exist.

Playboy Mar 69

The winner is one who knows when to drop out in order to get in touch.

Quoted by Peter Newman "The Table Talk of Marshall McLuhan" *Maclean's* Jun 71**LANGUAGE:** ENGLISHView: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#) [PREVIOUS](#) 15 of 18 [NEXT](#) [Text Only](#) | [Download](#) | [Fax](#) | [Email](#)
[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : **Collected Quotations**Terms: **privacy** ([Edit Search](#))

View: Full

Date/Time: Wednesday, July 5, 2000 - 6:07 PM EDT

[Search](#) | [Search Advisor](#) | [Get a Document](#) | [Check a Citation](#)
[ECLIPSE\(TM\)](#) | [History](#) | [Change Client](#) | [Options](#) | [Feedback](#) | [Sign Off](#) | [Help](#)
[About LEXIS-NEXIS](#) | [Terms and Conditions](#)

Copyright © 2000 LEXIS-NEXIS Group. All rights reserved.

lexis.com™

[Change Client](#) [Options](#) [Feedback](#) [Sign Off](#) [Help](#)[Search▶](#) [Search Advisor▶](#) [Get a Document▶](#) [Check a Citation▶](#)[ECLIPSE™](#) [History](#)View: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)[◀ PREVIOUS](#) 18 of 18 [NEXT ▶](#)[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : **Collected Quotations**Terms: **privacy** ([Edit Search](#))*Copyright 1988 Simpson's Contemporary Quotations*Copyright 1988 James B. Simpson
Simpson's Contemporary Quotations**SECTION:** Communication & The Arts**SUBJECT:** Radio & Television; Observers & Critics**LENGTH:** 44 words**SOURCE:** Louis Kronenberger**QUOTE:**

For tens of millions of people [television] has become habit-forming, brain-softening, taste-degrading.

The Cart and the Horse Knopf 64**Privacy** was in sufficient danger before TV appeared, and TV has given it its death blow.
*ib***LANGUAGE:** ENGLISHView: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)[◀ PREVIOUS](#) 18 of 18 [NEXT ▶](#)[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : **Collected Quotations**Terms: **privacy** ([Edit Search](#))

View: Full

Date/Time: Wednesday, July 5, 2000 - 6:08 PM EDT

[Search](#) | [Search Advisor](#) | [Get a Document](#) | [Check a Citation](#)
[ECLIPSE\(TM\)](#) | [History](#) | [Change Client](#) | [Options](#) | [Feedback](#) | [Sign Off](#) | [Help](#)
[About LEXIS-NEXIS](#) | [Terms and Conditions](#)

Copyright © 2000 LEXIS-NEXIS Group. All rights reserved.

lexis.com™

[Change Client](#) [Options](#) [Feedback](#) [Sign Off](#) [Help](#)[Search](#) [Search Advisor](#) [Get a Document](#) [Check a Citation](#)[ECLIPSE™](#) [History](#)View: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)[1 of 4](#) [NEXT](#)[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : [Collected Quotations](#)Terms: **fourth amendment** ([Edit Search](#))*Copyright 1988 Simpson's Contemporary Quotations*

Copyright 1988 James B. Simpson
Simpson's Contemporary Quotations

SECTION: The World**SUBJECT:** Law; Judicial Opinions**LENGTH:** 231 words**SOURCE:** Sandra Day O'Connor, Associate Justice, US Supreme Court**QUOTE:**

A moment of silence is not inherently religious.

Concurring opinion in 6-3 ruling that an Alabama law authorizing voluntary prayer or meditation in public schools violated the 1st Amendment by encouraging religious practice, 4 Jun 85

It is difficult to discern a serious threat to religious liberty from a room of silent, thoughtful schoolchildren.

ib

Statutes authorizing unreasonable searches were the core concern of the framers of the **4th Amendment**.

Minority opinion in 5-4 ruling that broadened an exception to the **4th Amendment** rule barring use of unconstitutionally seized evidence in criminal trials, 9 Mar 87

It is a measure of the framers' fear that a passing majority might find it expedient to compromise **4th Amendment** values that these values were embodied in the Constitution itself.

ib

We hold that the reckless disregard for human life implicit in knowingly engaging in criminal activity known to carry a grave risk of death represents a highly culpable mental state . . . that may be taken into account in making a capital sentencing judgment when that conduct causes its natural, though also not inevitable, lethal result.

Majority opinion in 5-4 ruling that some accomplices in crimes leading to death may be executed even if they did not personally kill or intend to kill, 21 Apr 87

LANGUAGE: ENGLISHView: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)[1 of 4](#) [NEXT](#)[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : [Collected Quotations](#)Terms: **fourth amendment** ([Edit Search](#))

View: Full

Date/Time: Wednesday, July 5, 2000 - 6:09 PM EDT

lexis.com™

[Change Client](#) [Options](#) [Feedback](#) [Sign Off](#) [Help](#)[Search](#) [Search Advisor](#) [Get a Document](#) [Check a Citation](#)[ECLIPSE™](#) [History](#)View: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)[PREVIOUS](#) 4 of 4 [NEXT](#)[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™ - Narrow Results](#) | [Save As ECLIPSE](#) | [More Like This](#) | [More Like Selected Text](#)Source: [All Sources](#) : / . . . / : [Collected Quotations](#)Terms: **fourth amendment** ([Edit Search](#))*Copyright 1988 Simpson's Contemporary Quotations*Copyright 1988 James B. Simpson
Simpson's Contemporary Quotations**SECTION:** The World**SUBJECT:** Law; Judicial Opinions**LENGTH:** 916 words**SOURCE:** Potter Stewart, Associate Justice, US Supreme Court**QUOTE:**

It must always be remembered that what the Constitution forbids is not all searches and seizures, but unreasonable searches and seizures.

Majority opinion in 5-4 ruling that prohibited the federal government from using evidence improperly seized by state officials, 27 Jun 60

The **4th Amendment** and the personal rights it secures have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.

Unanimous opinion that Constitution bars police from electronic eavesdropping, 5 Mar 61

For me this is not something that can be swept under the rug and forgotten in the interest of forced Sunday togetherness.

Dissenting opinion in 6-3 ruling that upheld blue laws, 29 May 61

I shall not today attempt further to define the kinds of material . . . but I know it when I see it.

Concurring opinion in 6-3 ruling that overturned ban on pornographic films, 22 Jun 64

At the very least, the freedom that Congress is empowered to secure . . . includes the freedom to buy whatever a white man can buy, the right to live wherever a white man can live. If Congress cannot say that being a freeman means at least this much, then the 13th Amendment made a promise it cannot keep.

Majority opinion in 7-2 ruling that upheld a 102-year-old law prohibiting racial discrimination in the sale and rental of real estate, 17 Jun 68

The dichotomy between personal liberties and property rights is a false one. Property does not have rights. People have rights.

Majority opinion in 4-3 ruling that upheld a district court's refusal to hear a case involving property rights, 23 Mar 72

In fact, a fundamental interdependence exists between the personal right to liberty and the personal right in property.

ib

These death sentences are cruel and unusual in the same way that being struck by lightning is cruel and unusual.

-- **Voltaire**

21. One of the best temporary cures for pride and affection is seasickness; a man who wants to vomit never puts on airs.

-- **Josh Billings**

22. To be proud and inaccessible is to be timid and weak.

-- **Jean Baptiste Masillon**

23. Pride breakfasted with Plenty, dined with Poverty, supped with Infamy.

-- **Benjamin Franklin**

24. There is this paradox in pride--it makes some men ridiculous, but prevents others from becoming so.

-- **Charles Caleb Colton**

Privacy

25. Gentlemen do not read each other's mail.

-- **Henry L. Stimson**

26. Privacy is the right to be alone--the most comprehensive of rights, and the right most valued by civilized man.

-- **Louis D. Brandeis**

27. Modern Americans are so exposed, peered at, inquired about, and spied upon as to be increasingly without privacy--members of a ;naked society and denizens of a goldfish bowl.

-- **Edward V. Long**

28. Far from the madding crowd's ignoble strife.

-- **Thomas Gray**

29. Let there be spaces in your togetherness.

-- **Kahlil Gibran**

30. Don't draw another's bow, don't ride another's horse, don't mind another's business.

-- **Proverb**

Procrastination

31. Waiting is a trap. There will always be reasons to wait...The truth is, there are only two things in life, reasons and results, and reasons simply don't count.

-- **Robert Anthony**

CENTER FOR DEMOCRACY & TECHNOLOGY

Our Mission / Get Involved / Staff / Publications / Links / Search CDT / Jobs / Action!

July 3, 2000

Testimony, Speeches & Filings

The Fourth Amendment and the Internet

Testimony of James X. Dempsey
Senior Staff Counsel
Center for Democracy and Technology
<http://www.cdt.org>

before the
Subcommittee on the Constitution of the House Judiciary Committee

April 6, 2000

Mr. Chairman and Subcommittee Members, thank you for calling this hearing and affording CDT the opportunity to testify about Fourth Amendment protections in cyberspace. Our nation is at a point where revolutionary changes in communications and computer technology have outpaced the privacy protections in our laws. Far more information than ever before is available to the government under minimal or inadequate legal standards. It is time for Congress to strengthen the privacy laws to restore a balance between government surveillance and personal privacy, to build user trust and confidence in these economically vital new media, and to afford both law enforcement agencies and online service providers the clear guidance they deserve.

The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values on the Internet. Our core goals include ensuring that the Constitution's protections extend to the Internet and other digital information technologies. CDT also coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for more than 50 computer, communications, and public interest organizations, companies and associations working on information privacy and security issues.

The Internet is a wonderfully transformative medium. Consequently, it has become a necessity in most workplaces and a fixture in most schools and libraries. According to a December 1999 Harris poll, 56% of American adults are online, 6 times higher than 4 years ago. But as more and more of our lives are conducted online and more and more personal information is transmitted and stored electronically, the result has been a massive increase in the amount of sensitive data available to government investigators.

While the Justice Department frequently emphasizes the ways in which digital technologies pose new challenges to law enforcement, the fact is that, on balance, the digital revolution has been a boon to government surveillance and collection of information. The FBI estimates that over the next decade, given planned improvements in the digital collection and analysis of communications, the number of wiretaps will increase 300 per cent. Computer files are a rich source of evidence: in a single case last year, the FBI seized enough computer evidence to nearly fill the Library of Congress twice. As most people sense with growing unease, everywhere we go on the Internet we leave digital fingerprints, which can be tracked by marketers and government agencies alike. The FBI in its budget request for FY 2001 seeks additional funds to "data mine" these public and private sources of digital information for their intelligence value. Yet the computer and communications privacy laws were last updated in 1986.

Recently, following a series of hacker attacks on e-commerce web sites, the Justice Department has proposed changes to the electronic surveillance laws to enhance law enforcement authorities. (In fact, the changes are not directly responsive to the recent attacks, but have been on the Justice Department's agenda for some time.) But surely, before enacting any enhancements to government power, we should

ensure that current laws adequately protect privacy. As I will explain, the standards for government access to information are not high enough to protect the privacy of ordinary citizens. We must tighten the standards for government surveillance and access to information. CDT is prepared to work with the Congress and the Justice Department to flesh out the needed privacy enhancements, and to convene DPSWG as a forum for building consensus.

Background: Fourth Amendment Privacy Principles

To understand how far current privacy protections diverge from the principles of the Constitution, we should start with the protections accorded by the Fourth Amendment. If the government wants access to your papers or effects in your home or office, it has to meet a high standard:

- The government must obtain a warrant from a judge based on a showing of probable cause to believe that a crime has been, is being or is about to be committed and that the search will uncover evidence of the crime. The warrant must "particularly" describe the place to be searched and the things to be seized.
- The government must provide you with contemporaneous notice of the search and an inventory of items taken. *Richards v. Wisconsin*, 520 U.S. 385 (1997); *Wilson v. Arkansas*, 514 U.S. 927 (1995). The notice and inventory requirements provide protections that are crucial notwithstanding the existence of a judicial warrant. In the case where police have come to the wrong address, you can try to point that out to them and they may withdraw. If you are the subject of a lawful search, you can observe the police to ensure that they confine their search to the scope of the warrant. In the case of a prolonged search, you can even rush to the courthouse and ask a judge to stop or narrow the search. And the inventory allows you to seek return of your property and tells you what information is in the hands of the government, so that you can respond and defend yourself against the government's suspicions or allegations.

These rules apply in the computer age, so long as you keep information stored on your hard drive or disks in your home or office.

The Supreme Court held in 1967 that wiretapping is a search and seizure and that telephone conversations are entitled to protection under the Fourth Amendment. *Katz v. United States*, 389 U.S. 347 (1967), *Berger v. New York*, 388 U.S. 41 (1967). Congress responded by adopting Title III of the Omnibus Crime Control and Safe Streets Act of 1968, requiring a court order based on a finding of probable cause to intercept wire or oral (i.e., face-to-face) communications. 18 U.S.C. §2510 *et seq.* However, Congress did not require the contemporaneous notice normally accorded at the time of a search and seizure. This was a fateful decision, but, the government argued, to give contemporaneous notice would defeat the effectiveness of the surveillance technique. In part to make up for the absence of notice, and recognizing the other uniquely intrusive aspects of wiretapping, Congress added to Title III requirements that go beyond the protections of the Fourth Amendment. These additional protections included: permitting the use wiretaps only for investigations of a short list of very serious crimes; requiring high level Justice Department approval before court authorization can be sought; requiring law enforcement agencies to exhaust other, less intrusive techniques before turning to eavesdropping; directing them to minimize the interception of innocent conversations; providing for periodic judicial oversight of the progress of a wiretap; establishing a statutory suppression rule; and requiring detailed annual reports to be published on the number and nature of wiretaps.

Over time, though, many of these additional protections have been substantially watered down. The list of crimes has been expanded, from the initial 26 to nearly 100 today and more are added every Congress. Minimization is rarely enforced by the courts. The exhaustion requirement has been weakened. Evidence is rarely excluded for violations of the statute. Almost every year, the number of wiretaps goes up - 12% in 1998 alone. Judicial denials are rare - only 3 in the last 10 years. The average duration of wiretaps has doubled since 1988. So even in the world of plain old telephone service we have seen an erosion of privacy protections. The fragility of these standards is even more disconcerting when paired with the FBI's "Digital Storm" plans for digital collection, voice recognition and key word searching, which will reduce if not eliminate the practical constraints that have up to now limited the

volume of information that the government can intercept.

After it ruled that there was an expectation of privacy in communications, the Supreme Court took a step that had serious adverse consequences for privacy: It held that personal information given to a third party loses its Fourth Amendment protection. This rule was stated first in a case involving bank records, *United States v. Miller*, 425 U.S. 435 (1976), but it is wide-ranging and now serves as the basis for government access to all of the records that together constitute a profile of our lives, both online and offline: credit, medical, purchasing, travel, car rental, etc. In the absence of a specific statute, these records are available to law enforcement for the asking and can be compelled with a mere subpoena issued without meaningful judicial control. The implications of this "third party record" rule are seen most recently in the Administration's proposed Cyberspace Electronic Security Act (CESA), which would allow the government to obtain encryption "keys" or other decryption information from third parties under a court order procedure that would provide neither the probable cause nor the notice protections of the Fourth Amendment.

In 1979, a third piece of the privacy scheme was put in place when the Supreme Court held that there is no constitutionally-protected privacy interest in the numbers one dials to initiate a telephone call, data collected under a device known as a pen register. *Smith v. Maryland*, 442 U.S. 735, 742 (1979). While the Court was careful to limit the scope of its decision, and emphasized subsequently that pen registers collect only a very narrow range of information, the view has grown up that transactional data concerning communications is not constitutionally protected. Yet, in an increasingly connected world, a recording of every telephone number dialed and the source of every call received can provide a very complete picture - a profile - of a person's associations, habits, contacts, interests and activities. (Extending this to email and other electronic communications can, as I explain below, be even more revealing.)

In 1986, as cellular telephones service became available and email and other computer-to-computer communications were developing, Congress 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, 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 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 allow for public or congressional oversight through annual reports.

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 then:

- 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. Does this mean that information is being stored more and more in configurations not protected by the Fourth Amendment? The government argues that this is a choice people make - you can keep the data on your own server and you can stay off the Internet if you care about privacy. But isn't this a little like arguing that you lose your privacy rights when you choose to communicate using the services of a telephone company, and if you want to preserve your privacy you should visit the person and have a face-to-face conversation? To say that people are choosing to let go of their data and stop there would leave the Fourth Amendment protections available in the home when increasingly information is not stored there anymore. Rather, it is necessary to adopt legislative protections that map Fourth Amendment principles onto the new technology.

It is clear that the surveillance laws' protections are too weak:

- The standard for pen registers is minimal - judges must rubber stamp any application presented to them.
- Many of the protections in the wiretap law, including the special approval requirements and the statutory rule against use of illegally obtained evidence, do not apply to email and other Internet communications.
- Data stored on networks is not afforded full privacy protection.
- ISP customers are not entitled to notice when personal information is subpoenaed in civil lawsuits; notice of government requests can be delayed until it is too late to object.
- And inconsistent standards apply to government access to information about one's activities depending on the type of technology used. For example, watching the same movie via satellite, cable TV, Internet cable modem and video rental is subject to four different privacy standards.

In addition, there are many ambiguities, some of which have existed since ECPA was enacted, others caused by technology's continuing evolution since 1986. For example, does the pen register statute apply to email or Web communications? If so, what are "the numbers dialed or otherwise transmitted"? To get email addresses and Web addresses (URLs), can the government serve a pen register order on the ISP or must it use an order under ECPA? What information is collected under a pen register order and from whom in the case of a person who is using the Internet for voice communications? What standard applies if the person has a cable modem? Is an Internet portal an electronic communications service under ECPA? Are search terms covered by ECPA? Does ECPA cover government access to information about one's activity at an e-commerce site? Do people have a constitutionally protected privacy interest in their calendars stored on Internet Web sites? At best, the answers are unclear.

The importance of these questions is heightened by the fact that transactional or addressing data for electronic communications like email and Web browsing can be much more revealing than telephone numbers dialed. First, email addresses are more personally revealing than phone numbers because email addresses are unique to individual users. Furthermore, if the pen register authority applies to URLs or the names of files transmitted under a file transfer protocol, then the addressing information can actually convey the substance or purport of a communication.

Outlining the Necessary Privacy Enhancements

To update the privacy laws, Congress could start with the following issues:

- Increase the standard for pen registers. Under current law, a court order is required but the judge is a mere rubber stamp - the statute presently says that the judge "shall" approve any application signed by a prosecutor saying that the information sought is relevant to an investigation. Instead, the government should be required to justify its request and the order should issue only if the judge affirmatively finds that the government has shown that the information sought is relevant and material.
- Define and limit what personal information is disclosed to the government under a pen register or trap and trace order served on Internet service providers.
- Add electronic communications to the Title III exclusionary rule in 18 USC §2515 and add a similar rule to the section 2703 authority. This would prohibit the government from using improperly obtained information about electronic communications.
- Require notice and an opportunity to object when civil subpoenas seek personal information about Internet usage.
- Improve the notice requirement under ECPA to ensure that consumers receive notice whenever the government obtains information about their Internet transactions.
- Require statistical reports for §2703 disclosures, similar to the reports required under Title III.
- Make it clear that Internet queries are content, which cannot be disclosed without consent or a probable cause order.
- Provide enhanced protection for information on networks: probable cause for seizure without prior notice, opportunity to object for subpoena access.

Conclusion

We do not need a new Fourth Amendment for cyberspace. The one we have is good enough. But we need to recognize that people are conducting more and more of their lives online. They are storing increasing amounts of sensitive data on networks. They are using technology that can paint a full profile of their personal lives. The price tag for this technology should not include a loss of privacy. It should not be the end of the privacy debate to say that technological change takes information outside the protection of the Fourth Amendment as interpreted by the courts 25 years ago. Nor is it adequate to say that individuals are voluntarily surrendering their privacy by using new computer and communications technologies. What we need is to translate the Fourth Amendment's vision of limited government power and personal privacy to the global, decentralized, networked environment of the Internet.

House Rule XI, clause 2(g)(4) disclosure: Neither James X. Dempsey nor CDT has received any federal grant, contract, or subcontract in the current or preceding two fiscal years.

[Previous Headlines](#) | [Action](#) | [Legislative Tracking](#) | [CDT's Privacy Policy](#)
[Free Speech](#) | [Data Privacy](#) | [Wiretapping](#) | [Cryptography](#) | [Domain Names](#) | [International](#) | [Bandwidth](#) | [Security](#) | [Terrorism](#) | [Authentication](#) |
[Right to Know](#)

[Our Mission](#) / [Get Involved](#) / [Staff](#) / [Publications](#) / [Links](#) / [Search CDT](#) / [Jobs](#) / [Action!](#)

©2000 **The Center For Democracy & Technology**
1634 Eye Street NW, Suite 1100
Washington, DC 20006
(v) 202.637.9800
(f) 202.637.0968

Technical concerns about this site: webmaster@cdt.org
Concerns or opinions about issues: feedback@cdt.org



PRIVACY TOOL KIT

ACCESS TO AND USE AND DISCLOSURE OF ELECTRONIC MAIL ON COMPANY COMPUTER SYSTEMS

A TOOL KIT FOR FORMULATING
YOUR COMPANY'S POLICY

Prepared by
David R. Johnson
Wilmer, Cutler & Pickering
and
John Podesta
Podesta Associates, Inc.



ELECTRONIC
MESSAGING ASSOCIATION

ACCESS TO AND USE AND DISCLOSURE OF ELECTRONIC MAIL ON COMPANY COMPUTER SYSTEMS:

A TOOL KIT FOR FORMULATING YOUR COMPANY'S POLICY

Prepared for the
Electronic Messaging Association
by

David R. Johnson
Wilmer, Cutler & Pickering

John Podesta
Podesta Associates, Inc.



ELECTRONIC MESSAGING
ASSOCIATION

1655 North Fort Myer Drive, Suite 850 Arlington, VA 22209 USA • Tel. 703/524-5550 • Fax: 703/524-5558

X.400: S=info; O=ema; A=mci; C=us • Internet: info@ema.org

Contents

Introduction	1
Background — Key Questions	3
Key Question #1	3
Who has a stake in establishing a responsible policy regarding access to and disclosure of company electronic mail?	3
Key Question #2	7
What baseline legal rights and duties constrain any policy?	7
Key Question #3	9
What operational features of electronic communication systems should affect any policy on access, use and disclosure?	9
Key Question #4	11
What analogies can be used to help formulate a consistent set of policies?	11
Key Question #5	13
What criteria should be used to evaluate a proposed policy?	13
Key Question #6	15
Has your policy been disclosed in advance to all concerned?	15
Alternative Policies By Topic.....	17
Policy Topic #1	
Disclosure of company policy/agreement in advance	17
Policy Topic #2	
Permissible/Specially Regulated uses of the electronic mail system.....	19
Policy Topic #3	
Monitoring for security violations	23
Policy Topic #4	
Grounds required for targeted access	25
Policy Topic #5	
Limitations on disclosure and use of information obtained by means of access or monitoring	27
Selected Policy Drafts	31
Policy Emphasizing “Official Use Only” and No Restraint on Access or Disclosure	31
Policy Allowing Access for Any Legitimate Business Purpose	33
Policy Emphasizing Employee’s Privacy Interest but Permitting Access on a Case-by-Case Basis	35
Policy Establishing Bright Line Rules Preventing Particular Types of Access and Disclosure and Requiring Notice and/or Approval by Employees.	37

Formulation of Your Policies	39
Who Should Participate?	39
What Assets Should Be Considered in Formulating Workplace Privacy Policies?	39
Information You May Want to Gather in the Course of Formulating Your Policy	39
Short Form Checklists	41
Glossary	43
Electronic Messaging Association	45

Introduction

The Electronic Messaging Association requested the preparation of this White Paper as a means of helping companies to decide what policies they should adopt with respect to access to and use and disclosure of electronic mail sent and received by their employees on company electronic mail systems.

The issues that need to be considered include the privacy rights of employees, the need of the employer to protect system security and manage company resources, the rights of third parties to get access to company files, and a range of other issues.

There is no single, simple answer to the policy questions relating to company electronic mail privacy. The key to successful handling of the issues is to consider them carefully and to reach a balanced judgment based on all applicable circumstances, particularly including your company's overall policies regarding workplace privacy with regard to paper files, phone calls, employee work spaces, and so forth.

Appropriate company policy will differ depending on the needs of the company, the reasonable expectations of employees, the rights of outsiders, and a balancing of various complex interests.

Most employers should establish privacy policies that deal with all media of communication used by employees, rather than singling out electronic mail as if it posed some unique threat to employee privacy.

The only policy that can be vigorously endorsed for virtually all circumstances is:

A company should have a policy to protect its employees' privacy, and it should tell employees what that policy is.

To help you formulate a company policy that is best suited to the particular circumstances of your business, this memo sets forth a series of key questions which should be considered in the course of formulating a policy. These key questions are followed by a series of alternative policy formulations which have been arranged by topic to help you tailor your policy regarding particular issues.

Finally, the memo sets forth portions of four selected sets of alternative policy drafts. These are not meant to be complete policy statements, but will illustrate how particular provisions might fit together.

To formulate a policy, most companies will find it useful to assemble a working group of company personnel who represent different interests and responsibilities. In addition to the company's chief information officer, corporate counsel and human resources personnel should participate in the formulation of policy and review policy drafts.



Background Key Questions

Key Question #1

Who has a stake in establishing a responsible policy regarding access to and disclosure of company electronic mail?

Although it is useful to think about the impact of policies on particular parties, you should keep in mind that the interests of employers, employees and third parties do not necessarily conflict. For example, both employers and employees have an interest in protecting the privacy of personnel records and in facilitating access to files needed to conduct the employee's business. You should also keep in mind that company electronic mail may not exist in isolation but may indeed be connected by gateways to the computer systems of other parties. Finally, electronic mail policy should be considered in the context of overall workplace privacy policies.

A. The employer

How will the policy affect:

- The employer's need to manage use of its computer systems?
- The employer's need to maintain a secure work place?
- The employer's need to prevent unlawful actions by employees?
- The employer's need to create a work environment in which employee productivity and morale is enhanced?
- The employer's need to exercise appropriate levels of supervision over employee's work?
- The employer's need to comply with any legal duty regarding employee privacy?
- The employer's right to privacy with regard to its business activities?
- The employer's need to offer guidance for supervisory and managerial employees?
- The employer's need to comply with any duty to prevent or provide third parties access to company communications?

B. The employee

How will the policy affect:

- The employee's need for a well functioning, congenial and secure workplace?
- The employee's stake in the success of the company's business activities?
- The employee's expectations that certain kinds of communications may be conducted in a confidential fashion?
- The employee's desire to know in advance how access to, use and disclosure of his/her communications will be treated by the company?
- The employee's need for guidance in dealing with electronic mail not intended for the employee?

C. Third parties

How will the policy affect:

- Third parties who have a need or duty to disclose their electronic mail messages to other parties?
- Third parties, using the company electronic mail system, who need to understand how their messages may be dealt with or disclosed within the company and to other third parties?
- Third parties to whom employees send personal messages?
- Third parties who have a legal right and need to discover company documents?
- Third parties who need access to company files to verify the course of dealing with the company?

D. Law enforcement authorities

How will the policy affect:

- Law enforcement officials who need to access company electronic mail records in connection with investigation of a crime?
- Law enforcement officials who seek access to company records in connection with

civil litigation or regulatory proceedings?

- Law enforcement officials who want to know who has a right to consent to the disclosure of any particular document?

E. Electronic Communications Service Providers

If company electronic mail is provided by a third party, whether by means of individual accounts issued to employees and paid for by the company or by means of supplying the infrastructure for an online system that appears to be available only to the company, the third party service provider has an interest in assuring that the policies followed by the company comply with the Service Provider's own rules.

How will company policy affect:

- The Service Provider's need to comply with applicable law?
- The Service Provider's interest in knowing who may give consent for access to and disclosure of electronic mail sent over its system by company employees?
- The Service Provider's goodwill?

Key Question #2

What baseline legal rights and duties constrain any policy?

- A. Duties not to invade employee privacy, in general
- Federal law does not establish a general right to privacy in the work place.
 - Some states, including California, may provide a legal right to privacy. Note: In some cases a message may be carried between two or more states; the company should carefully consider which state laws apply.
 - Some collective bargaining agreements may provide for some protections of privacy.
 - Some states' laws regarding employment practices have a public policy aspect that may impact privacy interests.
- B. Federal and State Law duties regarding use, interception, access during storage, and disclosure of electronic communications without authority.
- Duties to supply information to auditors, third parties in litigation, governmental regulators and law enforcement officials.
 - Tax consequences of allowing employees to use electronic mail systems for personal purposes.
 - Duties not to use information to defame, or portray in a false light, the sender or recipient of an electronic mail message.
 - A company may access and consent to disclosure of its own communications. As with other forms of communication, various employee communications may or may not be company communications.
 - A company providing electronic communications service to the public may not intercept or disclose communications on systems provided to the public, unless the company obtains consent, has a need to protect security or property, is legally considered to be the sender or an intended recipient, or otherwise comes within an established exemption.

The Electronic Communications Privacy Act (ECPA): Passed by Congress in 1986, ECPA extended to electronic communications protections roughly comparable to those extended by wiretap laws—at least with respect to unauthorized access by outsiders and to disclosure of private electronic mail by service providers offering electronic mail messaging to the public.

ECPA allows access to and disclosure of electronic mail messages with the consent of senders and recipients and as necessary to protect security or the service provider.

ECPA does make an important distinction based on whether or not the service provider offers communications service TO THE PUBLIC. Service providers offering to the public violate the law if they disclose private electronic mail messages without authorization from the sender or intended recipient, unless certain exemptions apply.

Source: *Protecting Electronic Messaging: The Electronic Communications Privacy Act of 1986*, Electronic Messaging Association

Key Question #3

What operational features of electronic communication systems should affect any policy on access, use and disclosure?

- Electronic mail is typically stored pending receipt.
- Electronic mail may easily be stored, for convenience, after receipt.
- Electronic mail may easily be forwarded.
- Erasing a message from personal files does not necessarily erase all copies of the message.
- Archival copies may be stored for substantial periods.
- Electronic files are more easily transferred than paper files.
- Electronic mail systems can transmit company documents and can become the means by which company records are stored and exchanged.
- Electronic mail may include substantial “attachments” in electronic form, which may involve access considerations different from those applicable to the covering message.
- Insofar as electronic mail is stored in electronic files after receipt, it may present special problems with respect to proof of authenticity and content.
- Electronic mail systems may be networked to provide connections to other companies or individuals or to public access points.
- Company files can be transferred offsite by electronic mail.
- Electronic mail may be sent to groups.
- Electronic mail is faster and more reliable than regular interoffice mail and will be relied upon more and more for transmission of messages.
- Electronic mail tends to substitute for telephone communications and therefore elicit less formal communications than are found in paper memoranda.
- Even if personal use of electronic mail on a company system is forbidden, it is likely to continue.

-
- Electronic mail systems are typically password protected, so that the appearance to the user is that messages cannot readily be accessed by anyone other than the sender, intended recipients and authorized system administrators. If greater access is allowed, without prior notice, users may be surprised.
 - Computer viruses can spread via electronic mail systems.
 - Electronic files can be searched quickly and provide a means for sharing and finding information on a company-wide basis.
 - Records of electronic mail transactions may disclose patterns of employee activity.
 - Electronic mail can be monitored from a distance and without any indication that the monitoring is occurring.
 - Electronic mail can be encrypted.
 - Company electronic mail systems may be accessed by employees who are located at remote sites, including personal computers operated in the employee's home.
 - Use of electronic mail at remote sites may create records of company business on computers that are not owned by or subject to physical control by the company.

Key Question #4

What analogies can be used to help formulate a consistent set of policies?

You may want to analyze your policy choices by considering your reactions to the following roughly analogous situations:

- Action by a subordinate, peer or superior to access paper files to respond to a business crisis when the affected employee cannot be reached;
- Regularly reviewing files kept in filing cabinets by employees;
- Inspecting an employee's desk drawer;
- Tape recording a meeting between employees, with their consent;
- Tape recording a meeting between employees, without their knowledge;
- Intercepting or monitoring employee telephone calls;
- Demanding that employees send their supervisors copies of all business correspondence;
- Having a supervisor attend meeting between an employee and customers;
- Accessing phone mail messages addressed to employees;
- Opening and reading all messages sent by employees through internal company mail;
- Using telephone toll records to analyze marketing options and business operations;
- Inspecting employee offices for security purposes;
- Sorting through folders in central files in order to respond to a discovery request in litigation;
- Reviewing selected employee's files and telephone message slips in the course of a financial or legal audit;
- Checking telephone accounting records for unauthorized personal long distance phone calls;
- Monitoring keystrokes or other computer generated transactional records to measure employee productivity;

-
- Telling someone you are hanging up on a group telephone call but then staying on the line to overhear the conversation;
 - Inventorying the desk of a departed employee;
 - Observing who comes and goes from the building and with whom they meet;
 - Inspecting employee offices to look for books or equipment that should be returned;
 - Investigating reports by employees regarding abuse by other employees of company resources;
 - Monitoring rest rooms with closed circuit television to check for drug usage.

Key Question #5

What criteria should be used to evaluate a proposed policy?

A. Does the policy:

- maintain a productive work place?
- appropriately preserve the company's and employee's interests in the information and system resources?
- establish and honor clear expectations regarding privacy?
- provide for adequate security?
- appropriately protect the rights of third parties?
- comply with all legal conditions?

B. Is the policy likely to be followed in practice?

Key Question #6

Has your policy been disclosed in advance to all concerned?

Alternative Policies By Topic

This section is designed to help you formulate answers to the key questions raised in the previous section. Each of the five subsections below covers a different aspect of electronic mail policy by outlining alternative policy options. The memo also sets forth, in italics, possible text for a policy statement.

Policy Topic #1

Disclosure of company policy/agreement in advance

This is the only policy option to which this memorandum offers no alternatives.

The company should fully disclose its policy in advance.

The company may, of course, refuse to continue to employ those who do not agree to abide by and have their communications subject to access and disclosure under the terms of a reasonable policy.

The company should distribute the policy through regular channels for distribution of policy guidance to its managers and employees. In addition, as a company might with any new policy, it might consider obtaining explicit acknowledgment that the employee has read and will abide by the policy.

Text for Policy Statement Introduction

This memorandum sets forth the company's policy with regard to access to and disclosure of electronic mail messages sent or received by company employees with the use of the company electronic mail system.

It also sets forth policies on the proper use of the electronic mail system provided by the company.

The company intends to honor these policies but must reserve the right to change them at any time with such prior notice, if any, as may be required under the circumstances.

Policy Topic #2

Permissible/Specially Regulated uses of the electronic mail system

A. Allow/Disallow use for personal purposes

1. The electronic mail system provided at company expense may not be used to send personal messages.

The company electronic mail system may not be used to send any messages of a personal character.

You are to use the electronic mail system only on official business.

All messages are company records. The company reserves the right to access and disclose all messages sent over its electronic mail system for any purpose.

2. If the electronic mail system is used for sending personal messages, the employee waives any claims to privacy.

Incidental and occasional personal use of electronic mail is permitted within the company, but such messages will be treated no differently from other messages.

The company reserves the right to access and disclose all messages sent over its electronic mail system for any purpose.

3. If the electronic mail system is used to send, receive or store personal messages, the employee must take steps to password protect the message and store it in special, personal and protected areas.

If you use the company electronic mail system to send, receive or store personal or private messages, then you must take special steps to protect the privacy of such messages through such means as designation of the message as private, password protection, and/or storing them in special areas.

The company will attempt to honor the privacy of such areas by refraining from accessing them unless it has reasonable grounds to do so.

4. Electronic mail provided at company expense for employee use will not be inspected by anyone other than employee — without employee's permission.

The company provides electronic mail to employees, at company expense, for their use on company business and incidentally for personal purposes.

The company will not seek to obtain access to the contents of any employee's electronic mail files without the permission of the employee.

Employees should take steps to assure that company documents that should be available to other employees of the company are so available.

B. Allow/Disallow use by third parties (customers and suppliers)

1. Only company employees may use the company electronic mail system.
2. Customers and suppliers may use the electronic mail system with special authorization and subject to certain conditions.

The company electronic mail system may be used by customers, suppliers and other third parties under certain circumstances.

Third parties will only be given access to the company electronic mail system if they agree to abide by all applicable rules.

Always use care in addressing messages to make sure you do not inadvertently send a message meant only for company employees to outsiders.

3. The company electronic mail system is open to the public for communications between the company and the public.

The company electronic mail system provides a means by which members of the public may communicate with the company.

Messages sent between the company and members of the public may be used by the company for any business purpose.

Members of the public who subscribe to the company's electronic mail system will be informed of applicable rules and will be required to agree to company policies with respect to access to and disclosure of electronic mail messages.

4. The company electronic mail system can be used by third parties to communicate with each other.

The company's electronic mail system has been configured to permit messaging between authorized non-company users.

The contents of a communication between such third parties will not be accessed or disclosed, other than for security purposes, without prior notice to the third party.

Electronic Messaging Association

EMA was founded in 1983 (then as the Electronic Mail Association) by eight companies who saw the potential of electronic messaging to move business into the 21st century. Today, EMA is made up of over 400 user and vendor companies. Vendor members are involved in all phases of messaging including software development, mainframe and mini computers, LAN messaging products, and public networks. User members reflect the proliferation of electronic mail into diverse industries including petroleum, finance, health care and aerospace.

From the very beginning, EMA's mission has been to foster an environment of ubiquitous worldwide messaging. In order to accomplish this, EMA has developed a four prong approach: to serve as an information/education clearinghouse, to identify and develop positions on key issues, to take an advocacy role and to promote interoperability. EMA provides the forum for industry leaders to come together and discuss the development of technology, standards and issues pertinent to electronic messaging.

EMA has long been an active voice in the evolution of electronic messaging standards and addressing requirements. The completion of the X.400 interconnection agreements among major commercial vendors was facilitated by EMA, and was a milestone in the development of the messaging industry. Today, EMA continues to work as a catalyst for more efficient information transfer and seamless interconnections among all messaging environments, including both the Internet and X.400 communities.

EMA has also been a leader in shaping messaging industry public policy. From early meetings with the Federal Communications Commission on regulatory policies and work on the landmark Electronic Communications Privacy Act of 1986 to our current involvement with workplace privacy and data encryption legislation and the development of the new National Information Infrastructure, EMA continues to play a key role in the development of policy and legal issues for electronic messaging.

EMA's diverse user and vendor membership is the most complete resource for information on both the messaging industry and the issues which will affect its future. As the only trade association dedicated exclusively to electronic messaging, EMA's role will continue to expand in the coming years with the rapid growth of the industry. EMA is committed to supporting the development and improvement of electronic messaging and information exchange technology and standards throughout the world.

Electronic Messaging Association

1655 North Fort Myer Drive, Suite 850 Arlington, VA 22209 USA • Phone: 703/524-5550 • Fax: 703/524-5558

EasyLink, Envoy 100, GENie, MCI Mail, Pacific Bell, SprintMail: EMA • CompuServe: 70007,2377
Dialcom: 52PRD003 • IBM Mail Exchange: USEMA001 at IBMMAIL

GLOSSARY

Archival Records and Backup

Records of electronic mail communications kept for security, system backup purposes, or to preserve the contents of certain messages in the event of future dispute.

Some systems are set up to produce regular backups, on a daily, weekly and monthly basis. Deletion of a copy of an electronic message on the operational disk may not delete that same message as stored in an archival copy.

Copies made for system backup purposes may be distinguished from copies of electronic mail made by senders or recipients, in their own electronic storage areas, for other purposes.

Electronic Mail

Electronic Mail is the generic name for the non-interactive communication of text, data, images or voice messages between a sender and designated recipient(s) by systems utilizing telecommunications links.

Electronic mail is often distinguished from a "bulletin board" or open posting system in which messages may be left by topic but may not be addressed to specific individuals or, in any event, are not expected to be opened only by the addressee.

Electronic mail systems often require the sender and recipient to enter a password as a precondition to access.

Electronic mail systems may allow the user to send a document as an "attachment" or to transfer a binary file.

(See discussion of technical features of electronic mail systems in Section IIC.)

Local Area Network (LAN)

A Local Area Network, or LAN, is a set of connections between computers that provides the basis for some electronic mail systems. Most LANs are within a small geographic area and serve a single organization.

Typically, LAN electronic mail messages are stored on a file server (a storage device) on a local area network.

A LAN often has a system administrator with rights to access any file on the system, unless it is encrypted, and to change passwords and privileges.

Short Form Checklists

1. Access

- Is the company legally free to access the information?
- Is there some alternative and less intrusive means of obtaining the information?
- Would access violate a reasonable expectation of privacy on the employee's part?
- Is access legally required?
- Has the employee been informed of the access or is there sufficient reason not to have done so?
- Has the proposed action been disclosed to an appropriate group of managers and recorded in writing?
- Would the company be embarrassed to tell its employees about the decision to access?

2. Disclosure

- Is the company legally free to disclose the information?
- Would the disclosure serve a legitimate business interest?
- Is there a duty to a third party to make the disclosure?
- Will the disclosure do some harm to the employee?
- Can the disclosure be limited in some way so as to respect the privacy interests of the employee?
- Has any party affected by disclosure been notified, or was there some sound reason not to give such notice?

Formulation of Your Policies

Who Should Participate?

- Senior Management
- Human Resources
- Counsel
- Employee Users
- Security
- Union Representatives
- MIS/CIO

What Assets Should Be Considered in Formulating Workplace Privacy Policies?

- Paper Files Cabinets— (Central/Personal)
- Employee Offices/Desks
- LANs
- Hard Disks
- Floppy Disks
- Voice Mail
- Electronic Mail
- Telephones
- Call Accounting Records
- Audio Recording Equipment
- Paper Mail
- Closed Circuit Television

Information You May Want to Gather in the Course of Formulating Your Policy

- Number of electronic mail users
- Preexisting policy statements including general statements of privacy policy in employee handbooks
- Nature and extent of current of electronic mail system use for personal purposes
- Connection of electronic mail system through gateways to other systems
- Extent of access to system by customers, third parties or “the public”
- Nature of employee’s current expectations
- Ability and use of electronic mail system to transfer documents not generally viewed as messages
- Plans for changes to electronic mail system
- Contract(s) with electronic mail service providers
- Employment agreement provisions
- Current security procedures
- Capability of electronic mail system to allow encryption, special password protection or privacy indicator

This type of policy allows the company to be relatively sure it is fully honoring any employee's privacy rights, reduces employee objections to oppressive electronic supervision, and allows discipline against overzealous managers.

On the other hand, a policy of this type may increase the risk of a law suit if the policy is violated, may interfere with some security measures, and may create procedural barriers to actions otherwise required to facilitate business decisions, honor obligations to third parties, or protect employer property.

Policy Establishing Bright Line Rules Preventing Particular Types of Access and Disclosure and Requiring Notice and/or Approval by Employees.

A. Specific Provisions

This memorandum sets forth the company's policy with regard to access to, and disclosure of, electronic mail messages sent or received by company employees with the use of the company electronic mail system.

It also sets forth policies on the proper use of the electronic mail system provided by the company.

The company intends to honor these policies but must reserve the right to change them at any time with such prior notice as may be reasonable under the circumstances.

The company provides electronic mail to employees, at company expense, for their use on company business and incidentally for personal purposes.

The company will not seek to obtain access to the contents of any employee's electronic mail files without the permission of the employee.

Employees should take steps to assure that company documents that should be available to the employees of the company are so available.

Employees found to have engaged in "snooping" will be disciplined appropriately and may be terminated.

The company reserves the right to access and disclose the contents of employee electronic mail messages, but will do so without the permission of the employee sending the message (or an intended recipient) only insofar as it is required by law or by legal obligations to third parties to do so or in order to protect its interests in the event that it reasonably suspects that an employee has committed, or is committing, a crime that might be aimed at, or attributed to the company.

Employees shall not be disciplined, terminated or have the terms and conditions of their employment altered solely as a consequence of the contents of electronic communications they have sent, unless the monitoring or access that led to the review of the contents of the communications was disclosed to and agreed to by each employee in advance.

B. Considerations

A policy that precludes certain types of access or disclosure without the permission of employees using the electronic mail system will tend to create the greatest expectations of privacy and will be easier to apply as a set of "bright line" tests.

without such approval is a breach of company policy for which employees will be disciplined. Access solely for the purpose of assuring system security may be approved in advance by security personnel.

B. Considerations

This policy recognizes employee expectations of privacy, and provides specific procedures to override those expectations, allows reasonable case-by-case balancing of interests and should help to reduce employee complaints.

This type of policy creates an atmosphere of trust, without preventing actions the employer may find necessary to protect its rights or honor duties to third parties.

On the other hand, this type of policy tends to require the employer to follow more elaborate and potentially costly procedures. Failure to comply with the expected procedures could itself become the basis of a complaint. And this type of policy tends to create expectations of privacy, to encourage the sending of private messages and therefore to create greater risks of surprise and dispute if access and disclosure become necessary.

Policy Emphasizing Employee's Privacy Interest but Permitting Access on a Case-by-Case Basis

A. Specific Provisions

This memorandum sets forth the company's policy with regard to access to, and disclosure of, electronic mail messages sent or received by company employees.

It also sets forth policies on the proper use of the electronic mail system provided by the company.

The company intends to honor these policies but must reserve the right to change them at any time.

The company recognizes that employees have a substantial interest in, and reasonable expectations of, privacy with regard to the electronic mail messages they send or receive, even when those messages involve only company business.

The company reserves the right to access and disclose the contents of employee electronic mail messages, but will do so only when it has a legitimate business need to do so and the urgency of the need is sufficiently strong to offset the company's commitment to honor the employee's interest in privacy.

The company will not monitor electronic mail messages as a routine matter.

The company may inspect the contents of electronic mail messages in the course of an investigation triggered by indications of impropriety or as necessary to locate substantive information that is not more readily available by some other means.

Electronic "snooping" by any employee is a violation of company policy and grounds for dismissal.

If you use the company electronic mail system to send, receive, or store personal messages, then you must take special steps to protect the privacy of such messages through such means as: designation of the message as private; password protection; and/or storing them in special areas.

Third parties will only be given access to the company electronic mail system if they agree to abide by all applicable rules.

The company reserves the right to disclose any electronic mail message to law enforcement officials. The company will give prior notice of such disclosure to employees who have sent or received such messages, unless the company believes that it may have been a victim of a crime, or has a legal obligation not to do so.

[] will review any request for access to the contents of electronic mail. Such requests must be approved in advance and any access undertaken

Policy Allowing Access for Any Legitimate Business Purpose

A. Specific Provisions

This memorandum sets forth the company's policy with regard to access to and disclosure of electronic mail messages sent or received by company employees.

It also sets forth policies on the proper use of the electronic mail system provided by the company.

The company intends to honor these policies but must reserve the right to change them at any time.

The company reserves the right to access and disclose the contents of employee electronic mail messages, but will do so only when it has a legitimate business need to do so.

The company will not monitor electronic mail messages as a routine matter.

Electronic "snooping" by any employee is a violation of company policy and grounds for dismissal.

Incidental and occasional personal use of electronic mail is permitted within the company, but such messages will be treated no differently from other messages.

Third parties will only be given access to the company electronic mail system if they agree to abide by all applicable rules.

The company reserves the right to disclose any electronic mail message to law enforcement officials.

B. Considerations

This policy allows employer access to employee electronic mail without consent when necessary for a legitimate business purpose (e.g., the unavailability of the employee).

This type of policy helps to create an atmosphere of trust, without preventing actions the employer may find necessary to further its legitimate business purposes.

On the other hand, failure to comply with the stated limitations on access could itself become the basis of a complaint. And this policy might not allow a more careful balancing of privacy interests and employer needs.

Selected Policy Drafts

To provide further guidance, the following drafts pull together particular provisions that could assist in formulating a consistent policy. Considerations bearing on the selection of these sets of policies are also discussed. In no case do these drafts purport to be full and complete policy drafts. They should be used in conjunction with formulating policies applicable in general to workplace privacy.

Policy Emphasizing “Official Use Only” and No Restraint on Access or Disclosure

A. Specific Provisions

This memorandum sets forth the company’s policy with regard to access to and disclosure of electronic mail messages sent or received by company employees with the use of the company electronic mail system.

It also sets forth policies on the proper use of the electronic mail system provided by the company.

The company reserves the right to change them at any time.

You are to use the electronic mail system only on official business.

All messages are company records. The company reserves the right to access and disclose all messages sent over its electronic mail system for any purpose.

Supervisors may review the electronic mail communications of the employees they supervise to determine whether there have been any breaches of security, violations of company policy, or defalcations of duty on the part of employees.

The company reserves the right to disclose any electronic mail message to law enforcement officials without any prior notice to any employees who may have sent or received such messages.

B. Considerations

A policy generally restricting employee use of the company electronic mail system to official use, and making no promises that the contents of electronic mail will be protected against access or disclosure for company purposes, has the lowest risk of creating reasonable expectations that personal electronic mail messages may be sent and protected.

This type of policy preserves company computing resources, allows maximum flexibility in enforcement measures, and reduces the risk that access or disclosure will violate legal rights of employees.

On the other hand, policies of this type may not actually prevent personal use of the electronic mail system, may encourage access and disclosure under circumstances giving rise to controversy and may not optimize employee’s sense that he is being trusted.

-
2. Any access must be reviewed and approved in advance by a high level employee.

[A high level employee] _____ will review any request for access to the contents of electronic mail to be made by the company without the consent of a sender or recipient.

3. Any access must be reviewed and approved in advance by more than one high level employee.

Two (or more) high level employees will review any request for access to the contents of electronic mail to be made by the company without the consent of a sender or recipient.

Such requests must be approved in advance and any access undertaken without such approval is a breach of company policy for which employees will be disciplined.

Access solely for the purposes of assuring system security may be approved in advance by security personnel.

4. Any use or disclosure of information obtained during approved monitoring or access must be reviewed and approved in advance by specified authorities.

The use or disclosure of information obtained from inspection or monitoring of company electronic mail must be reviewed and approved in advance by [Specified employee or committee].

-
3. Attempt to respect employee objection based on inclusion of purely personal information

The company will attempt to honor any employee's objection to the disclosure of the contents of an electronic mail message sent by such employee where such objection is reasonable based on the claim that the contents of such message are personal and private in nature, unless such disclosure is required to serve an important business purpose or comply with a legal obligation.

The company will attempt to remove the personal portions of company records to the extent feasible prior to disclosure.

- C. Disclosure and use of information regarding the parties to electronic communications

1. Use and disclosure of detailed information regarding the recipients and originators of electronic mail for any proper business purpose

The company may use information regarding the number, sender, recipient and addresses of messages sent over the electronic mail system for any proper business purpose.

- D. Limitations on disclosures to law enforcement officials

Any policy section dealing with disclosure to law enforcement officials should draw upon, and be consistent with, other existing policies established by the company with respect to cooperation with law enforcement regarding inspection of paper files and searches of physical spaces. When considering aspects of such policies that may deal with electronic messages, the company should attend to the following issues: 1) whether notice should be given to an employee when law enforcement officials seek access to messages addressed to the employee or under the employee's control; 2) whether any duty of the company to give notice depends upon the question whether law enforcement activity relates to the possibility that the company may be the victim of a crime; 3) whether the company commits itself to give notice unless law enforcement officials obtain formal orders prohibiting such notice (or, conversely, whether the company reserves the right to decide to cooperate with informal requests from law enforcement officials that notice not be given in a particular instance); and 4) whether the company will resist making disclosure to law enforcement officials of electronic messages addressed to, or under control of, a particular employee, without the employee's consent, unless required by law to make such disclosure.

- E. Special procedures to approve access, disclosure or use

1. No special procedure required provided other policies are followed.

Policy Topic #5

Limitations on disclosure and use of information obtained by means of access or monitoring

A. Limitations on internal use of contents of communications

1. No limit on internal disclosure of contents

The contents of electronic mail, properly obtained for legitimate business purposes, may be disclosed within the company without the permission of the employee.

2. Internal disclosure of contents to be limited to employees with reasonable need to know

The contents of electronic mail, properly obtained for legitimate business purposes, may be disclosed within the company without the permission of the employee. But any internal disclosure without the consent of the employee who sent the message shall be limited to those employees who have some reasonable need for access to the information.

3. Internal disclosure of contents to be limited to maximum feasible extent

The contents of electronic mail, properly obtained for legitimate business purposes, may be disclosed within the company without the permission of the employee. But any internal disclosure without the consent of the employee who sent the message shall be limited to the maximum feasible extent consistent with the company's needs.

B. Disclosure of contents of communications to third parties over the objection of a party to the communication

1. Disclosure to serve company purposes regardless of nature of employee objection

The company may disclose the contents of electronic mail messages sent to, or received by, company employees for any business purpose.

2. Attempt to respect employee objection based on personal embarrassment

The company may disclose the contents of electronic mail messages sent to, or received by, company employees for any business purpose.

The company will attempt to refrain from disclosure of particular messages, based on objections on the ground that publication of the message will create personal embarrassment for the employee who sent the message, unless such disclosure is required to serve an important business purpose or satisfy a legal obligation.

The employee consents to access by the employer to protect system security or the company's property rights.

The company will not access files marked personal, or stored in private file areas, without such good cause to do so.

F. No business purpose sufficient to permit access unless required by law

The company recognizes that employees have a substantial interest in, and reasonable expectations of, privacy with regard to the electronic mail messages they send or receive, even on electronic mail systems provided by the company.

The company reserves the right to access and disclose the contents of employee electronic mail messages, but will do so only insofar as it is required by law or by legal obligations to third parties to do so or in order to protect its interests in the event it reasonably suspects that the employee has committed or is committing a crime that might be aimed at or attributable to the company.

Policy Topic #4
Grounds required for targeted access

A. Any purpose

The company reserves and intends to exercise the right to access the contents of electronic mail communications for any business purpose.

The electronic mail system is provided by the company for employee use. It should be treated like shared filing systems—with the expectation that messages sent on company business or with the use of company facilities will be available for review by any authorized representative of the company for any purpose related to company business.

B. Any legitimate business purpose

The company reserves the right to access and disclose the contents of employee electronic mail messages, but will do so only when it has a legitimate business need to do so.

C. Business purpose and no other readily available means to obtain the information

The company recognizes that employees have some reasonable expectations of privacy with regard to the electronic mail messages they send or receive, even when those messages involve only company business.

The company reserves the right to access and disclose the contents of employee electronic mail messages, but will do so only when it has a legitimate business need to do so and the necessary information cannot be obtained with the employee's consent from any other more readily accessible source.

D. Business purpose sufficiently urgent to offset substantial employee interest in privacy

The company recognizes that employees have a substantial interest in, and reasonable expectations of, privacy with regard to the electronic mail messages they send or receive, even when those messages involve only company business.

The company reserves the right to access and disclose the contents of employee electronic mail messages, but will do so only when it has a legitimate business need to do so and the urgency of the need is sufficiently strong to offset the company's commitment to honor the employee's interest in privacy.

E. Reason to suspect violation of policy or security

The company may access and disclose the contents of electronic mail messages sent or received by company employees whenever it judges that such access or disclosure may be required to investigate a breach of the security of the electronic mail system.

E. No regular monitoring

The company will not monitor electronic mail messages as a routine matter.

The company will respond to legal process and fulfill its obligations to third parties.

The company will inspect the contents of electronic mail messages in the course of an investigation triggered by indications of impropriety or as necessary to locate substantive information that is not more readily available by some other less intrusive means.

Policy Topic #3

Monitoring for security violations

A. Regular monitoring by supervisors

Supervisors may review the electronic mail communications of the employees they supervise to determine whether there have been any breaches of security, violations of company policy, or defalcations of duty on the part of the employees.

B. Automated monitoring with inspection of contents

The company will use computer programs that monitor electronic mail messages, checking for particular words or patterns of activity, for purposes of assuring system security and compliance with company policies.

Supervisors may inspect the contents of electronic messages disclosed in the course of such monitoring or any follow up investigation, if such inspection is necessary to serve a business purpose.

C. Automated monitoring with limited inspection of contents

The company will use computer programs that monitor electronic mail messages electronically, checking for particular words or patterns of activity, for purposes of assuring system security and compliance with company policies.

D. Regular monitoring by system operators, with duty to report any apparent security breaches or violations of law and to avoid inappropriate or unnecessary investigations of personal communications.

System operators will regularly monitor electronic mail communications looking for any breach in security, violations of law, or infringement of company rules.

If system operators come across messages that appear to be private and personal in nature, and that do not appear to involve any violation of law or company rules, they will desist from inspection of such messages and will not disclose them to others.

If system operators find indications of illegal activity or violations of company policy or security, they will investigate further and/or report the messages and their findings to their superiors, as appropriate.

-
- C. Electronic mail system may not be used for “snooping”.

It is a violation of company policy for any employee, including system administrators and supervisors, to use the electronic mail and computer systems to satisfy idle curiosity about the affairs of others, with no substantial business purpose for obtaining access to the files or communications of others.

Employees found to have engaged in such “snooping” will be disciplined appropriately and may be terminated.

- D. Miscellaneous special uses.

You may want to consider adopting more specific policies dealing with the particular uses of electronic mail identified below.

- Use of the electronic mail system to send chain letters;
- Use of the electronic mail system to send copies of documents in violation of copyright laws;
- Receipt and “opening” of misaddressed electronic mail;
- Forwarding of electronic mail messages without a legitimate business purpose under circumstances likely to lead to embarrassment of the sender or to violate clearly expressed desire of the sender to restrict additional dissemination;
- Access to electronic mail sent by an employee to him or herself;
- Use of the electronic mail system or access to specific types of messages by retired or terminated employees;
- Special rules applicable to Electronic Data Interchange systems;
- Use of electronic mail systems for “moonlighting” or job searches;
- Use of electronic mail systems to send messages, access to which is restricted by government security laws or regulations.

1ST ITEM of Level 1 printed in FULL format.

Copyright (c) 1997 Albany Law Journal of Science &
Technology
Albany Law Journal of Science & Technology

1997

8 Alb. L.J. Sci. & Tech. 65

637
9800

Legal Notes

LENGTH: 27533 words

ARTICLE: COMMUNICATIONS PRIVACY IN THE DIGITAL AGE: REVITALIZING THE FEDERAL
WIRETAP LAWS TO ENHANCE PRIVACY

not

James X. Dempsey

* Senior Staff Counsel, Center for Democracy and Technology, Washington, D.C.
<www.cdt.org>. I am grateful to Jerry Berman, Joel Bernstein, Emilio Cividanes,
Geoff Feiss, Wallace Henderson, Kate Martin, Lynn McNulty, Ronald Plesser, and
Daniel Weitzner, who provided valuable comments on an earlier version of this
article, and to Adam White Scoville, for able research assistance. For a
lifetime's worth of inspiration, I am indebted to former Rep. Don Edwards,
longtime chairman of the Subcommittee on Civil and Constitutional Rights of the
House Judiciary Committee, for whom I had the privilege to work as assistant
counsel for a decade as he endeavored to enhance the civil rights and civil
liberties of all Americans.

SUMMARY:

... The ongoing worldwide revolution in communications technology is
fundamentally changing the way people conduct their business and private lives.
... Sections IV through IX apply these themes to specific policy issues:
(Section IV) the legal status of Internet communications and records stored
digitally in cyberspace; (Section V) implementation of the 1994 federal
legislation imposing surveillance assistance requirements on telecommunications
carriers; (Section VI) the role of encryption; (Section VII) protection of
wireless communications; (Section VIII) revisions, including those sought by the
Communication Administration, in the laws governing wiretaps, pen registers and "trap
and trace" devices; and (Section IX) emerging issues concerning law enforcement
cooperation and privacy protection in the international arena. ... While some
technological developments have made electronic surveillance easier, more
intrusive or more revealing, the FBI in the early 1990's began to complain about
the ways in which technological developments were making law enforcement
interception more difficult. ... The plain language of CALEA and the legislative
history indicate that "call-identifying information" means the numbers dialed by
a subscriber to direct a communication, or other signaling information that
serves the same call routing purpose as the dialed digits. ... Changes in
technology since 1994 when Congress adopted the CALEA legislation pose equally
difficult problems, while also creating opportunities for enhancing privacy. ...

TEXT:

[*67]

That the individual shall have full protection in person and in property is a

principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. n1

-----Footnotes-----

n1. Louis D. Brandeis & Samuel D. Warren, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

-----End Footnotes-----

I. Introduction

The ongoing worldwide revolution in communications technology is fundamentally changing the way people conduct their business and private lives. These changes are producing challenges for both privacy and law enforcement interests, stretching the limits of existing legal rules. Striking the proper balance between privacy and law enforcement in the electronic realm has always been a complex endeavor. Changes in communications technology have required periodic reexamination of privacy protections and law enforcement capabilities. It is time again for such a review.

There are broad grounds for concern that modern systems of communication are not private. Despite the convenience and the widespread popularity of cellular and other wireless telephones, they are notoriously insecure. n2 The open, networked nature of the Internet, while the source of its power as a medium, also makes it uniquely vulnerable. n3 Electronic communications systems generate vast quantities of transactional data that can be readily collected and analyzed. n4 The globalization of communications infrastructures threatens to turn the Bill of Rights into a local ordinance.

-----Footnotes-----

n2. Adam Clymer, Gingrich Is Heard Urging Tactics in Ethics Case, N.Y. Times, 10, 1997, at A1. See also Cellular Privacy: Is Anyone Listening? You Hear: Oversight Hearing before the Subcomm. on Telecommunications, Trade, and Consumer Protection of the House Comm. on Commerce, 105th Cong. Feb. 5, 1997 [hereinafter Cellular Privacy Hearing].

n3. Committee to Study National Cryptography Policy, National Research Council, Cryptography's Role in Securing the Information Society (Kenneth W. Dam & Herbert S. Lin eds. 1996) [hereinafter NRC Report].

n4. See Joel R. Reidenberg, Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?, 44 Fed. Comm. L.J. 195 (1992).

-----End Footnotes-----

Meanwhile, law enforcement agencies, particularly at the federal level, are putting increasing emphasis on electronic surveillance. n5 The use of year-long wiretaps on multiple individuals in the "Pizza Connection" drug trafficking case, the "Ill Wind" defense procurement fraud investigation, and the "Operation [*68] Polar Cap" money laundering investigation is seen as representing the

future of law enforcement. n6 Louis Freeh, Director of the Federal Bureau of Investigation (FBI), has called wiretapping "one of law enforcement's most valuable investigative techniques." n7 Freeh argues that wiretapping is crucial to investigation of cases involving terrorism, espionage, organized crime, drug trafficking, public corruption, and violent crime. n8 Without this technique, Freeh has testified, "law enforcement at the Federal, State, and local levels will be crippled." n9 Not surprisingly, therefore, a number of public policy debates in recent years have centered around law enforcement proposals to preserve or expand government surveillance capabilities in light of technological developments.

-----Footnotes-----

n5. Jim McGee, Wiretapping Rises Sharply Under Clinton, Wash. Post, July 7, 1996, at A1.

n6. See U.S. Dep't of Justice & FBI, Report on a Study of the Use of Electronic Surveillance Prepared by the United States Department of Justice and the Federal Bureau of Investigation, as Required by Section 810 of the Antiterrorism and Effective Death Penalty Act of 1996, Submitted to the United States House of Representatives and the United States Senate 21-22 (July 1996) [hereinafter July 1996 Electronic Surveillance Report to Congress].

n7. Encryption, Key Recovery, and Privacy Protection in the Information Age: Hearings Before the Senate Comm. on the Judiciary, 105th Cong. (June 4, 1997) (testimony of Louis J. Freeh).

n8. See id. at 9-10.

n9. See Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103rd Cong. 6 (1994) [hereinafter Digital Telephony Hearings] (testimony of Louis J. Freeh).

-----End Footnotes-----

This article addresses the privacy issues raised by new communications and computer technologies and the needs of law enforcement. Section II summarizes the principles underlying the federal wiretap laws and questions whether those laws currently provide adequate protection to privacy in light of judicial interpretations and technological enhancements in surveillance capabilities. Section III addresses some of the broad implications of ongoing changes in communications technology for privacy and law enforcement and identifies five trends that should guide the development of privacy protections for the digital age. Sections IV through IX apply these themes to specific policy issues: (Section IV) the legal status of Internet communications and records stored digitally in cyberspace; (Section V) implementation of the 1994 federal legislation imposing surveillance assistance requirements [*69] on telecommunications carriers; n10 (Section VI) the role of encryption; (Section VII) protection of wireless communications; (Section VIII) revisions, including those sought by the Clinton Administration, in the laws governing wiretaps, pen registers and "trap and trace" devices; and (Section IX) emerging issues concerning law enforcement cooperation and privacy protection in the

international arena. Each of Sections IV through IX includes recommendations for strengthening privacy protections while preserving necessary law enforcement capabilities.

-----Footnotes-----

n10. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. 1001-1010 and scattered sections of 18 U.S.C. and 47 U.S.C.) [hereinafter CALEA].

-----End Footnotes-----

The focus of this article is limited to government access to communications and stored electronic data and attendant issues, deferring to others the consideration of important questions concerning the disposition of control over personal information as between employers and employees or between businesses and customers. n11

-----Footnotes-----

n11. See David N. King, Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap," 67 S. Cal. L. Rev. 441 (1994). See also Sandra Petersen, Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?, 48 Fed Comm. L.J. 163 (1995); Alan F. Westin, Privacy in the Workplace: How Well Does American Law Reflect American Values?, 72 Chi. Kent L. Rev. 271 (1996); Oscar H. Gandy, Jr., Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace, 1996 U. Chi. Legal F. 77 (1996); Thomas R. Greenberg, Comment, E-Mail And Voice Mail: Employee Privacy and the Federal Wiretap Statute, 44 Am. U. L. Rev. 219 (1994).

-----End Footnotes-----

II. Electronic Surveillance and the Need for Strong Privacy Protections

The tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques ... Both proponents and opponents of wiretapping and electronic surveillance agree that the present state of the law in this area is extremely unsatisfactory and that the Congress should act to clarify the resulting confusion. n12

-----Footnotes-----

n12. S. Rep. No. 90-1097, at 67 (1968) (Omnibus Crime Control and Safe Streets Act).

-----End Footnotes-----

A. The Legal Framework

In important ways, electronic surveillance has always posed greater threats to privacy than the physical searches and seizures [*70] that the Fourth Amendment was originally intended to cover. n13 To begin with, "electronic surveillance is almost inherently indiscriminate." n14 Interception of a telephone line provides to law enforcement all of the target's communications, whether they are relevant to the investigation or not, raising concerns about compliance with the particularity requirement in the Fourth Amendment and posing the risk of general searches. n15 In addition, electronic surveillance involves an on-going intrusion in a protected sphere, unlike the traditional search warrant, which authorizes only one intrusion, not a series of searches or a continuous surveillance. n16 Officers must execute a traditional search warrant with dispatch, not over a prolonged period of time. If they do not find what they were looking for in a home or office, they must leave promptly and obtain a separate order if they wish to return to search again. n17 Electronic surveillance, in contrast, continues around-the-clock for days or months. Finally, the usefulness of electronic surveillance depends on lack of notice to the suspect. n18 In the execution of the traditional search warrant, an announcement of authority and purpose ("knock and notice") is considered essential so that the person whose privacy is being invaded can observe any violation in the scope or conduct of the search and immediately seek a judicial order to halt or remedy any violations. n19 In contrast, wiretapping is conducted surreptitiously.

-----Footnotes-----

n13. "The 'indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments,' and imposes 'a heavier responsibility on this Court in its supervision of the fairness of procedures'" *Berger v. New York*, 388 U.S. 41, 56 (1967) (quoting *Osborn v. United States*, 385 U.S. 323, 329, n. 7 (1966)).

n14. *Lopez v. United States*, 373 U.S. 427, 463 (1963) (Brennan, J., dissenting).

n15. See *id.*; Standards Relating to Elec. Surveillance, Am. Bar Ass'n Project on Minimum Standards For Criminal Justice, 87-95 (Approved Draft, 1971).

n16. See *Berger*, 388 U.S. at 57, 59.

n17. See *id.* at 57.

n18. See *Lopez*, 373 U.S. at 463-64 (Brennan, J., dissenting).

n19. The Supreme Court has recently reaffirmed the centrality of knock and notice to the Fourth Amendment's protective scheme. See *Richards v. Wisconsin*, 117 S. Ct. 1416 (1997); *Wilson v. Arkansas*, 514 U.S. 927 (1995).

-----End Footnotes-----

In 1967, in the landmark *Berger* and *Katz* cases, the Supreme Court ruled that electronic surveillance was a search and seizure covered by the privacy protections of the Fourth Amendment. n20 In *Berger*, the Court condemned lengthy, continuous or indiscriminate electronic surveillances, but in *Katz*, the Court

indicated that a short surveillance, narrowly focused on interception of a few [*71] conversations, was constitutionally acceptable if approved by a judge in advance and based on a special showing of need. n21

-Footnotes-

n20. See Berger, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967).

n21. See Berger, 388 U.S. at 59; Katz, 389 U.S. at 354-59.

-End Footnotes-

Responding to the Supreme Court's Berger and Katz opinions and to the arguments of law enforcement that wiretapping was a vital weapon in the efforts against organized crime, n22 Congress, in 1968, authorized law enforcement wiretapping under a system of protections intended to compensate for the uniquely intrusive aspects of electronic surveillance. n23 According to the Senate report, the legislation had "as its dual purpose (1) protecting the privacy of wire and oral communications and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." n24 The wiretap provisions were enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, so the federal wiretap law is still referred to sometimes as "Title III." n25

-Footnotes-

n22. See Controlling Crime Through More Effective Law Enforcement: Hearings on S. 300, S. 552, S. 580, S. 674, S. 675, S. 678, S. 798, S. 824, S. 916, S. 917, S. 992, S. 1007, S. 1094, S. 1194, S. 1333, and S. 2050 Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary, 90th Cong. passim (1967).

n23. Pub. L. No. 90-351, tit. III, 82 Stat. 212 (codified as amended at 18 U.S.C. 2510-22 (1996)).

n24. S. Rep. No. 90-1097, at 66 (1968).

n25. States may authorize wiretapping under restrictions at least as strict as the federal law, and most have done so. See 18 U.S.C. 2516(2). As of December 31, 1996, forty-five jurisdictions (including the District of Columbia, Puerto Rico, and the Virgin Islands) had laws on the books authorizing wiretapping, while eight states (Alabama, Arkansas, Kentucky, Maine, Michigan, Montana, South Carolina, and Vermont) did not allow wiretapping by state and local police. See Statistics Div., Admin. Office of the United States Courts, 1996 Wiretap Rep. at 13 (1997) [hereinafter 1996 Wiretap Rep.]. Every year, about half of the states that do authorize wiretapping report not a single use of it by state and local law enforcement agencies, according to the annual Wiretap Reports of the Administrative Office of the United States Courts. In 1995, for example, over half of the states that authorized wiretapping (22 out of 40) did not utilize the technique (including, e.g., such large states as Illinois, Ohio, Oregon, Virginia, and Wisconsin). Statistics Div., Admin. Office of the United States Courts, 1995 Wiretap Rep. at 12 (1996).

-End Footnotes-

brief, the legislation Congress enacted in 1968 had the following contents: the content of wire communications could be seized by the government in criminal cases pursuant to a court order issued upon a finding of probable cause; n26 wiretapping would be otherwise outlawed; n27 wiretapping would be permitted [*72] only for specified crimes; n28 it would be authorized only as a last resort, when other investigative techniques would not work; n29 surveillance would be carried out in such a way as to "minimize" the interception of innocent conversations; n30 notice would be provided after the investigation had been concluded; n31 and there would be an opportunity prior to introduction of the evidence at any trial for an adversarial challenge to both the adequacy of the probable cause and the conduct of the wiretap. n32 "Minimization" was deemed essential to satisfy the Fourth Amendment's particularity requirement, compensating for the fact that law enforcement was receiving all of the target's communications, including those that were not evidence of a crime. n33 The showing of a special need, in the form of a lack of other reasonable means to obtain the information, was viewed as justification for the failure to provide advance or contemporaneous notice of the search. n34

- - - - -Footnotes- - - - -

n26. 18 U.S.C. 2518(3) (1996).

n27. 18 U.S.C. 2511 (1996).

n28. 18 U.S.C. 2516(2) (1996).

n29. 18 U.S.C. 2518(3)(c) (1996).

n30. 18 U.S.C. 2518(5) (1996).

n31. 18 U.S.C. 2518(8)(d) (1996).

n32. 18 U.S.C. 2518(9), (10) (1996).

n33. B. Clifford S. Fishman & Anne T. McKenna, Wiretapping And Eavesdropping 14-11, at 14-11 to 14-12 (2d ed. 1995) [hereinafter Fishman & McKenna]; James G. Carr, The Law Of Electronic Surveillance 5.7(a), at 5-28 to 5-31 (1986). See also Clifford S. Fishman, The "Minimization" Requirement in Electronic Surveillance: Title III, the Fourth Amendment, and the Dred Scott Decision, 28 Am. U. L. Rev. 315 (1979).

n34. S. Rep. No. 90-1097, at 66 (1968).

- - - - -End Footnotes- - - - -

In 1978, Congress regulated wiretapping in national security cases through another statute, the Foreign Intelligence Surveillance Act (FISA). n35 This law authorizes the government to carry out electronic surveillance in the United States upon obtaining a judicial order (from one of a panel of Article III judges designated by the Chief Justice) based upon a probable cause finding that the target is a foreign power or an agent of a foreign power. n36 FISA was intended to be used primarily in foreign intelligence and counter-intelligence cases and therefore did not offer some of the protections required under Title

III. n37 Most significantly, FISA does not require that the target ever be given notice of the surveil [*73] lance, even after the investigation is closed, unless the government seeks to use the results in a criminal prosecution. n38 In addition, for individuals who are not U.S. citizens or permanent resident aliens, the statute does not require probable cause to believe that the target is engaged in criminal conduct. Rather, it is enough that the target is an agent of a foreign power. n39 Even for U.S. citizens, the statute allows surveillance where there is probable cause to believe that the person is engaged in clandestine intelligence activities on behalf of a foreign power, "which activities involve or may involve a violation of the criminal statutes of the United States." n40

-Footnotes-

n35. Pub. L. No. 95-511, tit. I, 101, 92 Stat. 1783 (1983) (codified at 50 U.S.C. 1801-11 (1996)).

n36. 50 U.S.C. 1805(a)(3)(a).

n37. Foreign Intelligence Surveillance Act: Oversight Hearings before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary, 98th Cong. 2-18 (1983) (testimony of Mary Lawton).

n38. Cf. 50 U.S.C. 1806(c).

n39. 50 U.S.C. 1801(b)(1) (defining an "agent of a foreign power").

n40. Id. at 1801(b)(2)(A) (emphasis added).

-End Footnotes-

A third major piece of legislation regulating electronic surveillance was enacted in 1986, when Congress made an initial response to the emergence of wireless services and the digital era with the adoption of the Electronic Communications Privacy Act (ECPA). n41 Title III had been limited to voice communications, whether face-to-face or over a wire. ECPA extended Title III to include wireless voice communications and electronic communications of a non-voice nature, such as e-mail or other computer-to-computer transmissions. n42 ECPA was intended to reestablish the balance between privacy and law enforcement, which Congress found had been upset, to the detriment of privacy, by the development of communications and computer technology and changes in the structure of the telecommunications industry. Among the developments noted by Congress were "large-scale electronic mail operations, cellular and cordless phones, paging devices, miniaturized transmitters for radio surveillance, and a dazzling array of [*74] digitized networks." n43 Privacy, Congress concluded, was in danger of being gradually eroded as technology advanced. n44

-Footnotes-

n41. See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in sections of 18 U.S.C. including 2510-21, 2701-10, 3121-26).

n42. ECPA, in fact, did not extend all of Title III's protections to electronic communications. The court order authorizing the interception of

electronic communications can be based upon suspected violations of any federal felony, rather than the limited list of crimes that can serve as a predicate for telephone interceptions. See 18 U.S.C. 2516(3) (1996). In addition, no statutory exclusionary rule applies to non-voice interceptions that violate the procedures in federal law. See 18 U.S.C. 2515 (1996) (exclusionary rule only refers to wire or oral communications, not electronic communications).

n43. H.R. Rep. No. 99-647, at 18 (1986).

n44. S. Rep. No. 99-541, at 2-3, 5 (1986); H.R. Rep. No. 99-647, at 16-19 (1986). See also H.R. Rep. No. 99-647, at 18 (stating that "legal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology.").

- - - - -End Footnotes- - - - -

In addition to the twin goals of privacy and law enforcement, ECPA sought to advance a third goal: supporting the development and use of these new technologies and services. n45 Congress affirmatively wanted to encourage the proliferation of new communications technologies, but it recognized that consumers would not trust new technologies if the privacy of those using them was not protected. n46

- - - - -Footnotes- - - - -

n45. See S. Rep. No. 99-541, at 5 (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems").

n46. S. Rep. No. 99-541, at 5 (1986); H.R. Rep. No. 99-647, at 19 (1986).

- - - - -End Footnotes- - - - -

ECPA made it a crime to knowingly intercept wireless communications and e-mail, but authorized law enforcement to do so with a warrant issued on probable cause. n47 In ECPA, Congress also began to recognize the privacy implications of transactional data generated by communications systems. ECPA established rules for the use of pen registers, which capture numbers identifying outgoing calls, and for trap and trace devices, which capture numbers identifying incoming calls. n48 In addition, it set rules for law enforcement access to information identifying a subscriber of an electronic communications service. n49 ECPA also eased certain procedural requirements for interception of wire communications by federal law enforcement officers. n50

- - - - -Footnotes- - - - -

n47. 18 U.S.C. 2701-03 (1996).

n48. 18 U.S.C. 3121-27 (1996).

n49. 18 U.S.C. 2703(c).

n50. Pub. L. No. 99-508, 106, 100 Stat. 1848, 1856-57 (1986) (amending 18 U.S.C. 2518).

-----End Footnotes-----

When law enforcement officials discuss wiretapping today, they often hasten to emphasize how stringent are the privacy protections of the legal framework established between 1968 and 1986: that wiretaps are available only for the most serious cases; n51 that authorization to conduct a tap is sought only when all other investigative techniques have failed; n52 that applications are subject to [*75] rigorous judicial scrutiny; n53 that wiretaps are conducted in such a manner as to minimize the interception of innocent conversations; n54 and that parties whose conversations are intercepted are entitled to obtain after-the-fact judicial review of the authorization and conduct of wiretaps. n55 Law enforcement officials cite these protections as a way of reassuring legislators and the public that the intrusiveness of electronic surveillance is well regulated.

-----Footnotes-----

n51. See Digital Telephony Hearings, supra note 9, at 6, 8, 16-20 (testimony of Louis J. Freeh).

n52. See id. at 6, 8, 16, 22, 123.

n53. See id. at 16, 22.

n54. See id. at 22, 24.

n55. See id. at 16.

-----End Footnotes-----

B. Erosion of the Wiretap Laws' Protective Scheme

There is substantial evidence, however, technological developments aside, that the protections initially established in 1968 and reaffirmed in 1986 are not working as intended. It appears increasingly apparent that components of the balanced legislative scheme have been watered down by Congress itself and by the judiciary:

(1) Wiretapping is no longer confined to violent and major crimes. Although Congress recognized in 1968 that wiretapping was an extraordinary technique that should be used only for especially serious crimes, the list of offenses for which wiretapping is permitted has been expanded steadily ever since - from the original 26 in 1968 to 95 in 1996. n56 The original list was largely limited to espionage and treason, violent crimes, and offenses typically associated with organized crime. The current list has been so expanded that wiretapping is now authorized for cases involving false statements on passport applications and loan applications or involving "any depredation" against any property of the United States. n57 Further expansions are promoted in response to each new law enforcement concern that receives legislative attention. Wiretapping is used only rarely in cases involving homicide, kidnapping, or terrorism. In 1996, 71% of wiretaps nationwide were in drug cases. n58

-----Footnotes-----

n56. 18 U.S.C. 2516 (1996).

n57. Id.

1996 Wiretap Rep., supra note 25, at 8.

- - - - -End Footnotes- - - - -

(2) The yearly number of federal, state and local law enforcement wiretaps has gone up steadily, from 564 in 1980 to 1,149 in 1996. Wiretaps increased 9% in 1996 alone. n59 Judges rarely deny wiretap applications. In 1996, only one wiretap application was [*76] denied; 1,149 were approved. n60 For seven years in a row, 1989 through 1995, no judge, state or federal, denied a single government request for wiretapping. n61 In that period, judges approved 6,598 wiretap orders in criminal cases. n62 There has been equally dramatic growth in the use of pen registers and trap and trace devices. In 1995, the law enforcement agencies of the federal Justice Department alone executed 3,414 pen register orders covering the telephone facilities of 7,899 persons and 1,558 trap and trace orders affecting the telephones of 3,902 persons. n63 No judge has ever been known to deny an application for a pen register or trap and trace device, because the law states that a judge must approve any application signed by an Assistant United States Attorney (or higher-ranking government attorney) who certifies that the information likely to be obtained is relevant to an ongoing criminal investigation. n64

- - - - -Footnotes- - - - -

n59. Id. at 7.

n60. Id.

n61. Id. at 29.

n62. Id.

n63. Report on the Use of Pen Registers and Trap and Trace Devices by the Law Enforcement Agencies/Offices of the Department of Justice for Calendar Year 1996. Report submitted to the House and Senate Judiciary Committees, April 30, 1996 [hereinafter Pen Register Report].

n64. 18 U.S.C. 3123(a) (1996).

- - - - -End Footnotes- - - - -

(3) While Katz indicated approval of wiretaps of short duration, the longest wiretap in 1996 lasted 420 days. n65 The average length of intercepts has increased steadily, from an average of 21 days in 1980, to an average of 38 days in 1996. n66 The average number of calls intercepted per wiretap has also increased steadily, from 1,058 per intercept in 1980 to 1,969 in 1996. n67

- - - - -Footnotes- - - - -

n65. 1996 Wiretap Rep., supra note 25, at 8.

n66. See Statistics Div., Admin. Office of the United States Courts, 1990 Wiretap Rep. at 29 (1991); 1996 Wiretap Rep., supra note 25, at 29.

Id.

- - - - -End Footnotes- - - - -

(4) The courts authorize electronic surveillance even when law enforcement agencies have not exhausted all other reasonably available techniques. n68 In United States v. Garcia, n69 for example, the Eighth Circuit held that electronic surveillance approval does [*77] not require the exhaustion of all normal investigative techniques. n70 Representative of the judicial attitude is the conclusion of one court that the purpose of the statutory exhaustion requirement is "simply to inform the issuing judge of the difficulties involved in the use of conventional techniques." n71

- - - - -Footnotes- - - - -

n68. Fishman & McKenna, supra note 33, 8:47 at 8-96 to 8-97 & nn. 36-37 (citing United States v. Giordano, 416 U.S. 505, 515 (1974); United States v. Pacheco, 489 F.2d 554, 564-65 (5th Cir. 1974); People v. Milnes, 527 P.2d 1163, 1167 (Colo. 1974); Bell v. State, 429 A.2d 300, 302-04 (Md. Ct. Spec. App. 1981); Commonwealth v. Fenderson, 571 N.E.2d 11 (Mass. 1991); State v. Monsrud, 337 N.W.2d 652, 657 (Minn. 1983); State v. Lozano, 311 N.W.2d 529, 531 (Neb. 1981); People v. Versace, 426 N.Y.S.2d 61 (2d Dep't 1980); State v. Ahmadjian, 438 A.2d 1070, 1083 (R.I. 1981)).

n69. 785 F.2d 214, 223 (8th Cir. 1986).

n70. Id. at 223.

n71. See United States v. Pacheco, 489 F.2d 554, 564-65 (5th Cir. 1974).

- - - - -End Footnotes- - - - -

(5) The minimization requirement also has not been strictly enforced by the courts. n72 In Scott v. United States, n73 the Supreme Court held that the complete recording of all conversations on a phone line belonging to the woman with whom the subject of the order was living was acceptable. Law enforcement agents in that case had made essentially no efforts to minimize the interception of nonpertinent calls, despite the high proportion of calls on the line that were nonpertinent. The Court justified this pattern of recording on the ground that the subject often used coded language in very brief conversations. In Scott, 40% of the conversations intercepted were relevant, but the lower courts have read the case as effectively eliminating the requirement to minimize the recording of innocent conversations. Scott's impact is illustrated by United States v. Ozar, n74 where the Eighth Circuit upheld the "two minutes up/one minute down" technique recommended by the Justice Department, in which FBI agents listened to two out of every three minutes of every phone conversation. In Ozar, the government intercepted a total of 8,126 minutes of the defendant's telephone conversations, of which 223 minutes, or 2.75% were deemed pertinent to the ensuing charges. The Court of Appeals held that this was not a violation of Title III, not because the conversations were short and coded, as in Scott, but because they were lengthy and complicated. n75

-----Footnotes-----

n72. Fishman & McKenna, supra note 33, 14-4 at 14-8 to 14-11; Robert Plotkin, Bringing the Code: Excluding Illegal Wiretap Evidence, 10 BNA Criminal Practice Manual 432 (1996).

n73. 436 U.S. 128 (1978).

n74. Ozar v. United States, 50 F.3d 1440, 1448 (8th Cir. 1995), cert. denied, 116 S.Ct. 193 (1995).

n75. Id. at 1447-48.

-----End Footnotes-----

(6) Defendants' after-the-fact challenges to the authorization or conduct of surveillance are rarely sustained. n76 Between 1985 and 1994, judges nationwide granted 138 suppression motions while denying 3,060, for a 4.3% suppression rate. n77

-----Footnotes-----

n76. Plotkin, supra note 72, at 432.

n77. Compiled from Wiretap Reports covering the years from 1985 through 1994.

-----End Footnotes-----

[*78]

(7) The FISA court in its entire seventeen-year history has never turned down a government electronic surveillance request. n78 Little is known publicly about these taps, but the Justice Department has released figures showing that in 1996, the FISA court issued a record 839 orders, up 20% from the prior year. n79 Meanwhile, FISA has been used increasingly in criminal cases, n80 for which it was not designed. The government does this by claiming that it is conducting parallel intelligence and criminal investigations and proceeds under the more flexible FISA standards. In another very troubling development, Congress recently authorized the use of FISA evidence in secret deportation proceedings, allowing the evidence to be introduced without disclosure to the respondent, thereby dispensing with one of the statute's key procedural protections. n81

-----Footnotes-----

n78. Jim McGee & Brian Duffy, Someone to Watch Over Us, Wash. Post Mag., June 23, 1996, at 9, 12.

n79. 67 Federation of Am. Scientists, Secrecy and Government Bulletin (May 1997) (citing April 18, 1997 U.S. Dep't of Justice report to Congress).

n80. McGee & Duffy, supra note 78, at 9, 13.

n81. Anti-Terrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 401, 110 Stat. 1214, 1262 (codified at 8 U.S.C. 1534(e)).

-----End Footnotes-----

Enhancements in Government Surveillance

In the long term, digital telephone technology will enhance the FBI's ability to collect, share and analyze information. Many of these enhancements will come without any FBI development effort, driven by consumer demand. n82

-Footnotes-

n82. FBI Budget Justification for FY 1992, at 67, reprinted in Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations for 1992: Hearings Before a Subcomm. of the House Committee on Appropriations, 102nd Cong. 738 (1991).

-End Footnotes-

In many ways, it is clear that this 1991 prediction by the FBI is coming true. While Section IV examines Congress' response to FBI concerns that new technology is making electronic surveillance harder, there are other ways in which new communications and computer technologies provide substantial advantages to law enforcement.

Wireless Services. In a host of circumstances where, in the past, persons would have used pay phones or not made a call at all, they now use cellular or other wireless phones, which are readily tapped at central switches. (It is normally far easier to identify a target's wireless service provider than it was to predict which pay phone he or she would use.) Proportionately more wireless phones [*79] are tapped by law enforcement than traditional wireline phones. n83 Indeed, law enforcement has been so quick to utilize this capability that in some urban areas cellular companies had been unable to accommodate simultaneously all of the law enforcement agencies seeking to tap cellular calls from mobile telephone switching offices, and therefore had to install additional capacity.

-Footnotes-

n83. Digital Telephony Hearings, supra note 9, at 152 (testimony of Thomas E. Wheeler).

-End Footnotes-

Location information. In the course of processing calls, many wireless communications systems collect information about the cell site (or the sector within a cell site) of the person making or receiving a call. Systems may even locate a cellular phone merely while it is turned on, even if it is not handling a call. n84 The technology is proceeding in the direction of providing more precise location information, a trend that has been boosted by the rulings of the Federal Communications Commission in its "E-911" (enhanced 911) proceeding, which requires service providers to develop a locator capability for medical emergency and rescue purposes. n85 Wireless phone location information can be

obtained by law enforcement. If it is a record collected and stored as part of the billing process, it can be obtained under current law by a mere subpoena. To obtain it in real-time, law enforcement agencies have been using court orders issued under 18 U.S.C. 2703 (d). In 1994, three of the four manufacturers of cellular switches had developed the software capability to deliver location information to law enforcement immediately upon call completion. n86

-----Footnotes-----

n84. Tim Friend, Using Cell Phones to Reach Out and Find Someone, USA Today, Dec. 16, 1997, at 6D; Albert Gidari, Locating Criminals by the Book, Cellular Bus., June 1996, at 70.

n85. In June 1996, the FCC adopted a Report and Order and Notice of Proposed Rulemaking in Docket 94-102, requiring wireless service providers to modify their systems within eighteen months to enable them to relay to public safety authorities the cell site location of 911 callers. Further, the FCC ordered carriers to take steps over the next five years to deploy the capability to provide latitude and longitude information locating wireless telephone callers within 125 meters. Finally, the FCC proposed requiring at the end of the five year period that covered carriers have the capability to locate a caller within a forty foot radius for longitude, latitude and altitude, thereby, for example, locating the caller within a tall building. In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys., FCC Docket No. 94-102, Report and Order and Further Notice of Proposed Rulemaking (last modified Jan. 2, 1997) [hereinafter FCC E-911 Order] available at <<http://www.fcc.gov/Bureaus/Wireless/Orders/1996/fcc96264.txt>>.

n86. Digital Telephony Hearings, supra note 9, at 152-54 (testimony of Thomas E. Wheeler).

-----End Footnotes-----

[*80]

E-mail and other on-line communications. E-mail is in some respects easier to intercept than regular mail. Indeed, since e-mail messages are often stored with the service provider for a period of time before they are read by the intended recipient (and even sometimes after they are read), e-mail is less transient than telephone calls and thus more vulnerable to interception. Law enforcement can intercept a person's e-mail and other Internet activity in real-time, by monitoring the phone line that serves as most people's connection to the Net. n87 This allows law enforcement, when it chooses to do so, to obtain an extraordinary window into a person's life. More readily, e-mail messages can be obtained from the host computer of the service provider. This is the method most commonly used by law enforcement to access e-mail. n88 In this way, e-mail interception is easier than telephone interception: while a person might have one telephone number at home, a different number at work, and another when traveling on business or vacation, most people have only one e-mail address to which all their e-mail is sent, and where it is all subject to being accessed by the government. n89

-----Footnotes-----

n87. See Michael J. Sniffen, First Computer Wiretap Produces Hacking Charge Against Argentine Student, Associated Press, Mar. 29, 1996 (where

communications through a major Harvard University computer were sifted in a search for patterns used by a suspected hacker); Gaylord Shaw, Wiretap Nets a Hacker: In a cyber-monitoring first, U.S. accuses Argentinian, Newsday, Mar. 30, 1996, at A6.

n88. See, e.g., United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996) (search warrant for e-mail served on America Online); United States v. Lamb, 945 F. Supp. 441 (N.D.N.Y. 1996).

n89. By lurking in online "chat rooms," law enforcement officers are able to monitor communications. See Graeme Zielinski, Tracking Pedophiles on Vast Internet No Easy Task, Chicago Tribune, July 6, 1997, at C1 ("In a sense, the Internet has proven a boon to investigators, said an FBI investigator. 'These guys used to be in some back shed somewhere. We couldn't get to them....Now we can get inside their minds.'").

- - - - -End Footnotes- - - - -

Remote monitoring. Technology has freed law enforcement intercepts of the constraints of geography. Agents monitoring wiretaps do not have to sit hunched in vans outside the target's house. Instead, the intercepted communications can be transported hundreds or thousands of miles to a monitoring facility at a law enforcement office. It is now common in investigations spanning multiple jurisdictions to establish a single monitoring plant and transmit there in real-time all intercepted conversations to be monitored, minimized, and recorded. The courts have held that a single federal judge can issue wiretap orders for telephones any [*81] where in the country, so long as the personnel listening to the conversations work in the judge's jurisdiction. n90 The Drug Enforcement Agency forwards intercepts from many different investigations to a central facility in Utah, where they are transcribed and translated by military personnel. n91

- - - - -Footnotes- - - - -

n90. United States v. Rodriguez, 968 F.2d 130, 135 (2d Cir. 1992).

n91. Jim McGee, Military Seeks Balance in Delicate Mission: The Drug War; As Movement Expands, Law and History are Basic Guidelines, Wash. Post, Nov. 29, 1996, at A1.

- - - - -End Footnotes- - - - -

Computer analysis. As noted above, law enforcement has recognized the informational richness of signaling and transactional information. Computer analysis is key to law enforcement exploitation of this data. Computers have made it possible for law enforcement agencies to analyze vast amounts of information about personal communications patterns far more easily. Pen registers, which recorded the numbers dialed on a particular phone line, have been superseded by multiline dialed number recorders, and these, in turn, have been computerized, allowing agencies to automatically search for revealing patterns of calls. The DEA has developed an integrated system called TOLLS that will electronically load telephone call data from dialed number recorders into a mainframe system for matching and analysis. n92 Further computer analytic developments may be around the corner. Voice recognition technology, for example, would free law enforcement from the most labor intensive aspects of

monitoring conversations, removing one of the biggest practical constraints on the number of interceptions made.

-Footnotes-

n92. David Burnham, Above the Law 159 (1996) (citing U.S. Dep't of Justice, 1994 Congressional Authorization and Budget Submission, vol. 2, DEA section, at 47).

-End Footnotes-

Title III allows law enforcement to take full advantage of these enhancements, requiring telephone companies, service providers and all other communications carriers to provide all technical assistance to law enforcement agencies seeking to carry out authorized interceptions. n93

-Footnotes-

n93. See 18 U.S.C. 2518(4) (1996).

-End Footnotes-

III. Five Broad Technological Trends Affect Privacy and Law Enforcement, Posing Challenges and Offering Opportunities

Telecommunications, of course, did not stand still after 1986. Indeed, the pace of change in technology and in the structure of the [*82] telecommunications industry accelerated and continues to accelerate. n94

-Footnotes-

n94. H.R. Rep. No. 103-827, pt.1, at 12 (1994) (report on CALEA).

-End Footnotes-

Behind the individual enhancements to surveillance capabilities identified above are five broad technological developments n95 that profoundly challenge the assumptions made by Congress in 1968 when it first established the rules for electronic surveillance, and in 1986 when it reaffirmed those assumptions:

-Footnotes-

n95. A list such as the one that follows cannot be comprehensive of the changes underway in the digital world. Others, for example, would point to the developing "convergence" among voice, data, and images as another major trend in telecommunications. However, the trends discussed here were identified because they seem to have major implications for government surveillance and privacy.

-End Footnotes-

(1) The dramatic development of the Internet has transformed all over again methods of gathering, processing and sharing of information, which had already been transformed by the computer itself. In 1981, fewer than 300 computers were linked to the Internet. n96 In 1986, when ECPA was enacted, there were about 50,000 computers linked to the Internet. n97 By June 1996, there were over 9.4 million host computers worldwide linked to the Internet. Including users who connect to the Internet via modem, some 40 million people worldwide can access the Internet. n98 In commercial terms, networking has had enormous implications. The average number of electronic point-of-sale transactions in the United States went from 38 per day in 1985 to 1.2 million per day in 1993. n99 Estimates for the potential of "Internet commerce" range up to "tens of billions of dollars by the turn of the century." n100

-Footnotes-

n96. Reno v. ACLU, 929 F. Supp. 824, 831 (E.D. Pa. 1996).

n97. Id. n98. Id.

n99. Office of Technology Assessment, Information Security and Privacy in Network Environments, 1-2 (1994).

n100. The White House, A Framework for Global Electronic Commerce, July 1, 1997, at 2 (the "Magaziner report").

-End Footnotes-

The Internet is not like the telephone system, or the mail, or mass media. Rather, the Internet combines a much broader range of functions, serving not only the one-on-one functions of the telephone and the mail, but also the information functions of TV, newspapers and the library; the artistic functions of a movie theater and a museum; the political functions of a town meeting hall; n101 the marketing and shopping functions of a mall; the [*83] organizing functions of door-to-door canvassing; n102 and the social, even romantic functions of a nightclub or coffee house. As an intentionally open system of linked computers, the Internet is inherently insecure. n103 The dramatic development of the Internet as a networked global communications medium and the expansion in the range of transactions that occur on-line have produced a qualitative change in the nature of communications and, accordingly, in the nature and amount of the information that is exposed to both lawful interception and illegal intrusion or misuse.

-Footnotes-

n101. U.S. Senate hearings have been broadcast live over the Internet. See e.g., <<http://www.crypto.com/events/072596/>>; <<http://www.crypto.com/events/062696/>>; <<http://www.hotwired.com/wiredside/96/25/stuff/senate.28.8.ram>>.

n102. Grassroots groups across the political spectrum use the Internet to inform, organize and galvanize. The "Encryption Policy Resource Page" features an "Adopt Your Legislator" campaign, connecting Internet users with information about their legislators' positions on the encryption issue. The page operates in conjunction with e-mail alerts to interested citizens so that they can contact their representatives when legislative action is imminent. The Encryption

Policy Resource Page: Adopt Your Legislator! (visited July 26, 1997)
 <<http://www.crypto.com/adopt>>.

NRC Report, supra note 3, at 300.

-----End Footnotes-----

(2) Signaling information has become an increasingly rich source of information about habits of association and commerce. Congress in 1968 n104 and again in 1986 n105 assumed that there were two categories of data: content (which would receive the highest protection) and a category of minimally revealing dialing or routing information. However, in recent years, transactional data has evolved into a third, hybrid type, providing detailed information about a person's habits of association and commerce. n106 Yet this "profiling" data was totally unprotected until 1986 and has since been subject only to the most minimal protection. (Congress again tightened the standard for access to certain e-mail addressing information in 1994, as discussed below in Section IV.) On the Internet, this data gives a rich picture of a person's life. n107 In a similar development in the area of voice communications, advanced signaling systems have also blurred the distinction [*84] between call-identifying information and call content. There is some concern that the development of packet switching may obliterate the distinction between signaling data and communications content. n108 In some cellular and other wireless telephone systems, this signaling data includes location information, potentially turning wireless phones into tracking devices. n109 Law enforcement is increasingly turning to transactional or signaling data as a source of investigative importance. n110

-----Footnotes-----

n104. See Omnibus Crime Control and Safe Streets Act of 1968, tit. III, Pub. L. No. 90-351, 802, 82 Stat. 212 (codified at 18 U.S.C. 2510-20).

n105. See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in sections of 18 U.S.C. including 2510-21, 2701-10, 3126).

n106. Digital Telephony Hearings, supra note 9, at 158, 160-61, 166-78 (testimony of Jerry Berman, including Expanded Protection for Online Transactional Information, memorandum of the Electronic Frontier Foundation).

n107. See, e.g., Alan Boyle, Eyes Are On You When You're Online (last modified Sept. 10, 1997) <<http://www.msnbc.com/news/34363.asp>>; Jeffrey Rothfeder, No Privacy on the Net, PC World, Feb. 1997, at 223; John M. Broder, Making America Safe for Electronic Commerce, N.Y. Times, June 22, 1997.

n108. See U.S. Congress, Office of Technology Assessment, Electronic Surveillance in a Digital Age, at 57-61 (July 1995) [hereinafter OTA Electronic Surveillance Report].

n109. Digital Telephony Hearings, supra note 9, at 33 (testimony of Louis J. Freeh), 154 (testimony of Thomas E. Wheeler), 158 (testimony of Jerry Berman); H.R. Rep. No. 103-827, pt. 1, at 17 (1994).

n110. See Pen Register Report, supra note 63.

- - - - -End Footnotes- - - - -

The rapid expansion of wireless services, which are increasingly used not just by the wealthy and in business applications, but by ordinary citizens for personal conversations, has made electronic communication almost totally flexible and constantly available, yet also more insecure. The number of wireless customers has gone from 92,000 in 1984 to 44 million by the end of 1996. n111 Moreover, wireless transmission is no longer important only for voice communication, but is becoming increasingly important for data transfer. Wireless modems and wireless local area networks are linking computers and transferring data that could include proprietary information, medical records, and financial data. n112 Wireless links are increasingly serving as gateways to the global information infrastructure. While offering attractive advantages of flexibility, wireless communications are less secure than traditional landline communications. n113

- - - - -Footnotes- - - - -

n111. United States Wireless Demographics (visited July 25, 1997) <<http://www.wow-com.com/professional/reference/CusDemog.cfm>> (citing Cellular Telecommunications Industry Association, Year-End 1996 Data Survey).

n112. See Maryam Alavi, Dick Tracy's Office : Business Applications of Wireless Technologies, in The Emerging World of Wireless Communications (Institute for Info. Studies ed., 1996). See generally, Boyle, supra note 107.

n113. See Cellular Privacy Hearing, supra note 2.

- - - - -End Footnotes- - - - -

(4) Control over technology has shifted away from the hands of government and a few monopolies. Telephony itself is now characterized by competition and rapid innovation, producing an environment with many new products, services and features, and many new service providers. State-of-the-art encryption technology is no longer subject to government monopoly. Users can now affirmatively choose encryption technology that will enhance their [*85] privacy and protect the security of their data against criminals. The Internet was designed from the outset as a decentralized medium for rapid transmission of information, and has evolved to a state of unprecedented openness. Barriers to participation are low; anyone with a computer and a modem can be a publisher. Services and even entirely new infrastructures are developing rapidly in response to user demands. n114 Government efforts to control the development and spread of technology become harder to sustain.

- - - - -Footnotes- - - - -

n114. For example, certificate authorities are developing to verify identity in the digital world. See generally A. Michael Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Or. L. Rev. 49 (1996).

- - - - -End Footnotes- - - - -

(5) The globalization of communications technology and networks is breaking down national borders. One of the great strengths of the Internet is that it can be as easy to send an e-mail message to New York as to Nairobi. The information infrastructure is now global, as are the markets for telecommunications products and services. On the one hand, the irrelevance of borders means that government controls over information and technology become harder to maintain. On the other hand, enforceable privacy protections have not yet emerged for the global information infrastructure.

The remainder of this article examines how these trends have affected the balance between privacy and law enforcement and how that balance can be re-established.

IV. Protecting "Papers" in Cyberspace - The Internet and the Fourth Amendment

ECPA was intended to establish rules for government surveillance in the digital world. In many respects, it has proven to be a durable statute. However, technology has evolved in ways not contemplated when ECPA was enacted. In drafting ECPA, Congress assumed that it would be adequate to extend to electronic communications the constitutional conclusion that underpinned Title III in 1968: that capture of electronic communications would not be an unreasonable intrusion if there were stringent ex parte judicial review before the fact, minimization during a search, and equally stringent adversarial review after the investigation had been completed. n115 That assumption, however, was made when few if any foresaw the development of the multiple forms of activity that are carried on today in "cyberspace." The interactive [*86] nature of the Internet, with the rapid emergence of features such as home banking, telecommuting and even telemedicine, has produced an environment in which many people spend hours each day "on-line." n116 In this context, to intercept all of a person's electronic communications means a lot more today than it did in 1968 or 1986. These developments call for an examination of the effectiveness and coverage of ECPA.

- - - - -Footnotes- - - - -

n115. See S. Rep. No. 99-541, at 2-3, 5 (1986).

n116. See generally, Paul Gilster, *Digital Literacy* (1997); Sherry Turkle, *Life On The Screen* (1995); Howard Rheingold, *The Virtual Community* (1993).

- - - - -End Footnotes- - - - -

A first step toward examining ECPA would be to assess how the rules it set for governmental access to e-mail and other computer communications are working. Unfortunately, however, there is no publicly available data on which to base such an assessment. While the wiretap provisions of Title III require very detailed reports on interception of voice communications and interception of e-mail in transit, there is no similar requirement for collecting and publishing information on the extent of government access to e-mail and other electronic communications while they are in storage with service providers incident to transmission, by far the easier and presumably the more common means of government's accessing electronic communications. n117 This deficiency should be corrected by amending ECPA to require that courts and prosecutors submit reports on orders sought and granted for electronic communication access under 18 U.S.C. 2703, for inclusion in the Administrative Office reports on wiretapping. Until

such a change can be enacted, Congressional committees should exercise their oversight authority to obtain such data from the federal agencies and the major service providers.

-----Footnotes-----

n117. Cf. 18 U.S.C. 2701 et seq.

-----End Footnotes-----

Another issue that needs to be re-addressed is whether one of the key protections established in 1968, the minimization rule, can be applied to non-voice communications. Minimization means that law enforcement is not supposed to record non-relevant communications. At the time ECPA was enacted, it was assumed that this was impossible in the e-mail context: law enforcement must get all the communications to and from a target, and read each one to determine if it is relevant. n118 In 1986, in fact, the Senate Judiciary Committee expressly addressed this concern and suggested that minimization should be conducted by the initial law [*87] enforcement officers who review the intercepted communications. The committee stated that "Those officials would delete all non-relevant material and disseminate to other officials only the information which is relevant to the investigation." n119 This solution has been criticized as unrealistic. n120 Actually, it is not that different from what happens in the case of ordinary telephone wiretaps, since the initial law enforcement personnel who monitor voice intercepts conduct an initial review of each conversation to decide whether to record it or not.

-----Footnotes-----

n118. Larry Downes, Electronic Communications and the Plain View Exception: More "Bad Physics," 7 Harv. J.L. & Tech. 241, 263-67 (1996).

n119. S. Rep. No. 99-541, at 31 (1986).

n120. Downes, supra note 118, at 267.

-----End Footnotes-----

Technology, however, may offer a solution, producing more effective minimization than is available in the context of voice communications. Whether law enforcement accesses e-mail from the telephone company (or access provider) while in transmission, or from an e-mail service provider while it is in storage incident to transmission, it may be relatively easy for the service provider to perform the minimization. The service provider can use screens or filters to select from the e-mail messages to or from parties identified in the order only those containing certain key words or phrases that would be identical to those used by monitors in the voice context. n121 As the investigation proceeds and law enforcement learns more about the patterns of the target, the interception can become more discriminating.

-----Footnotes-----

n121. Law enforcement already took this approach in one case involving interception of computer communications. See Sniffen, supra note 87.

-----End Footnotes-----

Another set of assumptions are being challenged by the profound changes coming as a result of the Internet. These concern the degree of protection for governmental access one can justifiably expect with respect to transactional records held by third parties. In 1976, the Supreme Court in *United States v. Miller* ruled that individuals had no constitutionally protected privacy interest in business records that were held by a third party. n122 Miller involved checks held by a bank, and the rationale of the case assumed a world of paper records, yet the holding in its broadest implications has been applied unquestioningly to the electronic world. Thus, in 1979, the Court in *Smith v. Maryland* ruled that the use of a pen register to collect the phone numbers dialed on a surveillanced line did not implicate Fourth Amendment interests. n123

-----Footnotes-----

n122. See 425 U.S. 435 (1976).

n123. See 442 U.S. 735 (1979).

-----End Footnotes-----

[*88]

ECPA responded to *Smith* by requiring a judicial order for pen registers and trap and trace devices. n124 For transactional information relating to e-mail and other electronic communications, ECPA required a subpoena, a warrant or a court order. n125 In 1994, Congress recognized that transactional data associated with e-mail and other computer communications was emerging as a hybrid form of data, somewhere between addressing information and content, and was becoming increasingly revealing of personal patterns of association. Therefore, Congress set a higher standard for access to transactional data regarding electronic communications and eliminated subpoena access. n126 Congress should examine the Justice Department's interpretation and application of the new standard to see if it is adequate or should be strengthened. Such an examination must give adequate attention to the communicative, associational nature of the transactional data itself in an online environment. (Congress should also strengthen the procedure for access to transactional records in the ordinary telephone context, a point discussed below in Section VIII.)

-----Footnotes-----

n124. 18 U.S.C. 3121 (1996).

n125. Pub. L. No. 99-508, 201, 100 Stat. 1862 (adding 18 U.S.C. 2703(c)).

n126. See 18 U.S.C. 2703(c) (1996).

-----End Footnotes-----

Finally, reexamination of ECPA must question the assumption that there is a distinction between the communication of content and its storage. In an era when people work for "virtual companies" and conduct personal, political and business lives in "cyberspace," that distinction is increasingly blurred. The growth of online commerce, politics and relationships, the shift to distributed,

networked computing, the growth of the World Wide Web as an information source, and the ready ability to encrypt records stored with third parties, call into question the application to the Internet of concepts developed for governmental access to business records in a relatively static, paper-based environment and may significantly change the legal notion of what is a reasonable expectation of privacy.

It is time to reconsider how the lines have been drawn between records entitled to full Fourth Amendment protection and records under Miller that fall outside the protection of the Fourth Amendment. There are now essentially three legal regimes for access to electronic data: (i) the traditional Fourth Amendment standard, for records stored on an individual's hard drive or floppy disks; (ii) the Title III-ECPA standard, for records in transmission; and (iii) a third standard, the scope of which is probably unclear, for [*89] records stored on a remote server, such as the research paper (or the diary) of a student stored on a university server or the records (including the personal correspondence) of an employee stored on the server of the employer. n127 As the third category of records expands because people find it more convenient to store records remotely, the legal ambiguity grows more significant. Are the records stored on such a server accessible by mere subpoena? Are they covered by the "remote computing" provisions of ECPA? n128 If the records were seized from the individual's hard drive or floppies using a warrant or subpoena, contemporaneous notice would be required. n129 If the records were seized in transmission, a court order would be required, but the interception could proceed secretly. n130 If the records were seized from a third party, notice might be delayed. n131 Do these distinctions make sense? Is the delay or denial of notice for stored records acceptable any longer? Conceptions of the Fourth Amendment developed in a 20th century world of paper records may not be applicable to 21st century technologies where many of our most important records are not "papers" in our "houses," but are "bytes" stored electronically and accessed remotely at "virtual" locations.

-Footnotes-

n127. See 18 U.S.C. 2701-2703 (1996).

n128. See 18 U.S.C. 2703.

n129. Standard Fourth Amendment practice requires notice, achieved by service of the warrant or subpoena on the person possessing the items to be seized or produced. Wayne R. La Fave, Search And Seizure, 4.1-4.13 (3d ed. 1996).

n130. See 18 U.S.C. 2511(2)(a)(ii) (1996).

n131. See 18 U.S.C. 2703(b).

-End Footnotes-

V. Preserving Government Surveillance Capabilities While Protecting Privacy and Encouraging Technological Innovation

While some technological developments have made electronic surveillance easier, more intrusive or more revealing, the FBI in the early 1990's began to complain about the ways in which technological developments were making law enforcement interception more difficult. n132 These difficulties were often encompassed by

the term "digital telephony," although digital transmission itself was not really the problem. In fact, there were a number of problems. Some of the difficulties related to the rapid growth of wireless systems, which are easily updated at the central switches but did not always have the capacity to update multiple [*90] surveillances. Others were related to the increased competition in the telecommunications industry, which meant that a target could use two or more service providers, making one-stop surveillance impossible. Some problems arose due to services and features that put more control in the hands of users. During the 1994 hearings, the FBI voiced concerns about a number of these problems, some of which existed in analog systems, but which had become more common in digital switches. Among them were problems intercepting calls rerouted through call forwarding services and the inability to identify the destination of calls made using a speed dialing feature. n133 Some problems had to do with physical changes in the networks. For example, the FBI anticipated increasing trouble in covertly isolating the communication stream associated with a particular target as multiplexed transmission technologies and fiber cables replaced the paired copper wires that traditionally had been associated uniquely with each customer. n134

-----Footnotes-----

n132. See Digital Telephony Hearings, supra note 9, at 5-6 (testimony of Louis J. Freeh).

n133. See id. at 121 (information submitted by Louis J. Freeh, "Technology-Based Problems Encountered by Federal, State, and Local Law Enforcement Agencies").

n134. See id. at 24 (testimony of Louis J. Freeh).

-----End Footnotes-----

Congress responded to these technological developments by enacting the Communications Assistance for Law Enforcement Act of 1994 (CALEA, sometimes referred to as the "digital telephony" legislation). n135 CALEA requires telephone companies to ensure that new technologies (and some old technologies) do not impede law enforcement interception of communications. n136 The legislation mandates, in effect, that carriers must take steps to ensure that the broad technological trends in the industry do not eliminate law enforcement access to communications of targeted individuals.

-----Footnotes-----

n135. Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. 1001-1010 and scattered sections of 18 U.S.C. and 47 U.S.C. (1994)).

n136. See id. at 103, 104.

-----End Footnotes-----

In adopting CALEA, Congress explicitly stated its intention to preserve the balance among the three interests that had guided the drafters of ECPA in 1986: law enforcement needs, privacy, and technological innovation. n137 Congress accepted the FBI's assurances that the legislation would preserve the status quo in terms of law enforcement surveillance, without expanding govern [*91]

ment capabilities. n138 Congress stressed specifically that the surveillance requirements of CALEA should be narrowly interpreted. n139 Congress also required carriers to change their systems to protect the privacy and security of communications not authorized to be intercepted. n140 To ensure that implementation did not block technological innovation, Congress prohibited the FBI from dictating network or equipment design standards. n141 Finally, Congress also amended some provisions of ECPA to heighten privacy protections. n142

-Footnotes-

n137. H.R. Rep. No. 103-827, pt. 1, at 22 (1994).

n138. When FBI Director Louis Freeh appeared before a joint hearing of the House and Senate Judiciary subcommittees in August 1994 to support the final version of CALEA, he stressed that the legislation would preserve wiretapping as it had existed since 1968:

Without question... court-authorized electronic surveillance is a critical law enforcement and public safety tool. I think we have reached a remarkable compromise and achievement in preserving that tool as it has existed since 1968 We believe that the legislation, as introduced this past Tuesday, offers the strongest investigative assurances that the authority which Congress gave us in 1968 will continue unimpeded by technology...

Digital Telephony Hearings, supra note 9, at 112-13. These assurances followed a series of statements of Director Freeh to the same effect at the March 18, 1994 hearing of the same subcommittees. Id. at 7, 9, 10, 16, 29-30, 14, 49.

n139. Congress stated as follows:

The Committee intends the assistance requirements in section 2602 to be both a floor and a ceiling. The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past. The Committee urges against overbroad interpretation of the requirements. The legislation gives industry, in consultation with law enforcement and subject to review by the FCC, a key role in developing the technical requirements and standards that will allow implementation of the requirements. The Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements.

H.R. Rep. No. 103-827 at 22-23.

n140. See H.R. Rep. No. 103-827, pt. 1, at 17; CALEA, 103(a)(4)(a) (codified at 47 U.S.C. 1002(a)(4)(a)).

n141. See CALEA, 103(b)(1) (codified at 47 U.S.C. 1002(b)(1)).

n142. See Pub. L. No. 103-414, 202-207.

- - - - -End Footnotes- - - - -

However, since CALEA was enacted, a struggle has been underway in which the FBI, on behalf of law enforcement generally, has attempted to broadly interpret the requirements of CALEA, by dictating system design and mandating, nationwide, certain capabilities in excess of traditional interception practices. n143 The most [*92] notable and troubling aspect of this campaign is the FBI's effort to use CALEA, in contravention of explicit assurances during the drafting process, to require cellular phone companies and other wireless service providers to have location tracking capability built into their systems for law enforcement purposes. n144 The FBI is also claiming, for example, that CALEA mandates interception of certain conference calls after the targeted facility has been dropped from the conversation, thus continuing the surveillance against parties and facilities for which no judicial approval was granted. n145 Seeking to exploit the increasing value of signaling information, the FBI has argued that CALEA requires the configuration and delivery of a signaling channel that includes detailed message notifications about the targeted facility. The FBI maintains that this configuration and delivery should be performed whether or not there is a call in progress and for facilities not identified in the surveillance order. n146 In a provision with far reaching implications, anticipating the adoption of packet switching protocols that could obliterate the distinction between signaling and content, n147 the FBI and industry have proposed allowing carriers to deliver communication content to law enforcement under a mere pen register order, depending once again on law enforcement to sort out the signaling information from the content. n148

- - - - -Footnotes- - - - -

n143. John Markoff, Telephone Industry Seeks Aid in Wiretap Battle with F.B.I., N.Y. Times, July 16, 1997, at A13; Jim McGee, FBI Calls for Greater Wiretap Capability, Phone Industry Pressed to Install New Surveillance Equipment, Wash. Post, Apr. 30, 1997, at C13; John Markoff, Dispute Arises Over Deal For Wiretaps, N.Y. Times, February 15, 1997, at 35; Seth Schiesel, Reduces Scope of Proposal on Wiretapping Phone Networks, N.Y. Times, Jan. 15, 1997, at A11; Jim McGee, Heightened Tensions Over Digital Taps, Wash. Post, Oct. 27, 1996, at H1; John Markoff, Cellular Industry Rejects U.S. Plan for Surveillance, N.Y. Times, Sept. 20, 1996, at A1; John Markoff, F.B.I. Wants Advanced System To Vastly Increase Wiretapping, N.Y. Times, Nov. 2, 1995, at A1.

n144. Telecommunications Industry Liaison Unit, FBI, Electronic Surveillance Interface Document, at 39, 50 (June 24, 1996) [hereinafter ESI Document].

n145. Id. at 17.

n146. Id. at 32 (feature status message providing updates whenever the subject alters a network-provided feature); 41 (surveillance status message indicating the status of the tap if the subject is not making or receiving a call); 36-37 (party hold and party join message); 32-33 (incoming call identifying message).

n147. See OTA Electronic Surveillance Report, supra note 108, at 57-61.

n148. Telecommunications Industry Assoc., Standards Proposal No. 3580-A, Proposed New Standard, "Lawfully Authorized Electronic Surveillance," 22-25 (Oct. 1, 1997) [hereinafter SP 3580-A].

- - - - -End Footnotes- - - - -

A. Congress' Legislative Mandate for Surveillance Features Was Premised on the Effective Enforcement of Strict Privacy Protections

CALEA was based on the dual premise that (i) Title III and other laws authorizing electronic surveillance have strict legal [*93] requirements and (ii) those requirements are being stringently enforced by the courts to protect privacy. As suggested above, this premise is becoming increasingly tenuous. If privacy protections afforded by the wiretap laws are not being strictly enforced, then the foundation of CALEA falters and the legislation becomes far more threatening, requiring as it does the ubiquitous adoption of features in the nation's telephone systems to ensure ready government access.

The premise of CALEA would also be negated by legislative weakening of the wiretap standards. Already the Justice Department has successfully won Congressional repeal of the provision extending ECPA to wireless data transfers. n149 The extension of ECPA to wireless data transfers was one of the privacy enhancements adopted in CALEA with the intent of balancing privacy concerns with law enforcement needs. n150 In addition, in its proposed anti-terrorism law forwarded to Congress in 1995, the Clinton Administration sought numerous weakening changes in Title III, including: (i) weakening the sanctions against illegal wiretapping, (ii) facilitating the procurement of roving taps and warrantless taps, n151 and (iii) creating exemptions from the carefully crafted privacy protection standards of the Foreign Intelligence Surveillance Act. n152 Although many of the Clinton changes were not enacted, the Justice Department has continued to pursue them and has proposed others that would loosen the privacy standards of the wiretap laws. n153

- - - - -Footnotes- - - - -

n149. See Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 731, 110 Stat. 1214, 1303 (amending 18 U.S.C. 2510(12)).

n150. See Pub. L. No. 104-414, 203.

n151. H. Rep. No. 105-896 (1997).

n152. See Pub. L. No. 104-132, 401, 110 Stat, 1214, 1258.

n153. See July 1996 Electronic Surveillance Report to Congress, supra note 6.

- - - - -End Footnotes- - - - -

As discussed in Section VIII, many of the proposed changes in the wiretap laws should be rejected on the merits. However, the fact that CALEA now requires telephone companies to design their systems to facilitate law enforcement surveillance is an additional reason to oppose any weakening of the wiretap standards. If the Executive Branch and Congress wish to fulfill the intent of

CALEA, they should strengthen, not weaken, the privacy protections of Title III, ECPA and FISA. Unless these laws, in light of judicial interpretation and continuing technological developments, offer meaningful protection to privacy, the foundations of CALEA will be eroded. [*94]

In CALEA, Congress Denied the Government Design Control and Mandated Privacy Protection

During the Bush Administration, the Justice Department urged Congress to adopt legislation that would have created de facto licensing authority over the development and deployment of new communications technology. n154 Telecommunications companies and civil liberties groups opposed the legislation, arguing that any legislation should be narrowly crafted to address identified problems while providing for public accountability and protecting privacy and not interfering with the innovation and competitiveness that have fueled the digital revolution. After hearings and consultations with industry, privacy groups, and law enforcement, Congress rejected the broad approach originally proposed by the FBI. Instead, with the strong support of the FBI, Congress enacted CALEA, which established minimum functional requirements intended to preserve rather than expand law enforcement access to communications, and deferred to industry to develop solutions. n155

-Footnotes-

n154. Digital Telephony Hearings, supra note 9, at 67 (prepared statement of Jerry Berman and Ronald L. Plesser); 71 (Interim Report of the Digital Privacy and Security Working Group on the FBI's Digital Telephony Proposals).

n155. Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. 1001 et seq. (1994)).

-End Footnotes-

CALEA requires telephone companies to design (and in some cases retrofit) their networks to ensure that law enforcement agencies can carry out electronic surveillance on advanced digital equipment and services. n156 Three of its four requirements are intended to preserve law enforcement access. These pertain to (1) the interception of call content; n157 (2) the interception of call-identifying information; n158 and (3) the delivery to law enforcement of intercepted call content and call-identifying information. n159 In contrast, the fourth requirement of CALEA, section 103(a)(4), requires carriers to protect the privacy and security of communications not authorized to be intercepted. n160

-Footnotes-

n156. 47 U.S.C. 1002(a).

n157. Id. at 1002(a)(1).

n158. Id. at 1002(a)(2).

n159. Id. at 1002(a)(3).

n160. Id. at 1002(a)(4).

-----End Footnotes-----

Congress intended that, in the first instance, common carriers and equipment manufacturers, not government agencies, would develop publicly the details for implementation of these assistance [*95] requirements. n161 Congress expected that this approach would temper law enforcement demands with considerations of privacy and innovation, as well as cost and competitiveness. If industry failed to produce a standard or if any agency or person had concerns about the standard, the legislation gave the Federal Communications Commission the authority to develop an appropriate standard, taking into account the need to protect privacy and to promote innovation. n162

-----Footnotes-----

n161. See H.R. Rep. No. 103-827, pt. 1, at 26 (1994).

n162. See CALEA, 107(b) (codified at 47 U.S.C. 1006(b)). See H.R. Rep. No. 103-827, pt. 1, at 27.

-----End Footnotes-----

A distinction should be drawn between what CALEA mandated as a minimum national standard for law enforcement access versus what expansions in surveillance capability will be available to law enforcement as a result of market-driven technological developments. Before CALEA, some changes in telecommunications technology were making law enforcement surveillance harder, while other changes were making surveillance easier or more productive. CALEA was intended to "preserve the status quo" by ensuring that technological developments did not erode law enforcement access to call content and identifying information. Congress did not intend to impede the development of technology that makes surveillance easier or more fruitful, nor did it intend to deny law enforcement the authority to take advantage of those developments. n163 Congress left intact the existing authority under 18 U.S.C. 2518(4), which authorizes law enforcement to take advantage of all technological developments enhancing surveillance capability and requires companies to make available whatever advanced capability they have. But Congress did not mandate the nationwide ubiquitous installation of every technologically possible surveillance enhancement. Instead, Congress mandated the nationwide availability only of certain minimum features, based upon its understanding of past surveillance practices as described in the CALEA hearings and based upon the FBI's description in the CALEA hearings of what its needs were. n164

-----Footnotes-----

n163. Congress did intend in CALEA to raise the legal standard for access to certain categories of information, including location information that was already available in some systems and transactional data associated with e-mail. See H.R. Rep. No. 103-827, pt. 1, at 17-18, 31-32.

n164. See H.R. Rep. No. 103-827, at 17-18, 31-32.

-----End Footnotes-----

[*96]

C. CALEA Implementation: Law Enforcement Efforts to Require Carriers to Provide Expanded Surveillance Capabilities

In respects, the checks and balances Congress wrote into CALEA have worked as intended. The FBI published in the Federal Register, under a notice and comment procedure, a capacity notice that was widely criticized and withdrawn. n165 The FBI published a second capacity notice revealing much more data about historical surveillance patterns, n166 but that second notice also raised serious questions which the Bureau must address in finalizing the capacity requirements. In terms of capability, industry bodies drafted "safe harbor" technical standards to provide the detail necessary to translate CALEA's broad functional requirements into network and equipment specifications. n167 The FBI had extensive input in the standards process, articulating law enforcement's desires and pushing hard for an expansive reading of the requirements.

-----Footnotes-----

n165. Implementation of the Communications Assistance for Law Enforcement Act, 60 Fed. Reg. 53643 (1995) (Initial Notice and Request for Comments).

n166. Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, 62 Fed. Reg. 1902 (1997) (Second Notice and Request for Comments).

n167. CALEA, 107(a) (codified at 47 U.S.C. 1006(a) (1994)).

-----End Footnotes-----

Unfortunately, the FBI's participation went beyond the consultation intended by Congress and instead amounted to an effort to dominate the standards process and dictate specific surveillance features. Nonetheless, as of October 1997, industry had largely rejected FBI demands for surveillance features that, in contravention of the clear intent of CALEA, would expand the government's electronic surveillance capability beyond its current reach. n168 In two respects, however, industry acceded to FBI demands for features that would go beyond the status quo.

-----Footnotes-----

n168. The House Judiciary Committee set forth its intent as follows:

The Committee intends the assistance requirements in section 2602 to be both a floor and a ceiling. The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past. The Committee urges against overbroad interpretation of the requirements....The Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements.

H.R. Rep. No. 103-827, at 22-23.

-----End Footnotes-----

(1) Location information. Industry yielded to FBI insistence that cellular and other wireless systems be designed to provide information on the location of their customers as they make and receive calls. This involves capturing and decoding signals to law enforcement the signals that identify a wireless telephone user's location for call processing purposes. n169 It is clear from the legislative history that Congress did not intend to impose geographic location information as a CALEA requirement with respect to cellular or other wireless systems. n170 Concerns with "location tracking" were initially a major source of opposition to the legislation, so the FBI was eager to disavow any interest in location information at an early stage. Thus, early in 1994, the FBI expressly assured Congress that CALEA did not mandate provision of location information, n171 and nothing in the legislative history suggests that any of the changes made as the legislation proceeded through the drafting process were intended to bring location information within the scope of CALEA requirements.

- - - - -Footnotes- - - - -

n169. See *Gidari*, supra note 84, at 70.

n170. "The bill requires telecommunications carriers to ensure their systems have the capability to... (2) Isolate expeditiously information identifying the originating and destination numbers of targeted communications, but not the physical location of targets " H.R. Rep. No. 103-827, pt. 1, at 16.

n171. In the hearings leading to enactment of CALEA, FBI Director Freeh testified that CALEA would not require carriers to make location information uniformly available. Freeh testified that "call setup information" (later "call-identifying information") listed as a CALEA requirement was not intended to include location information. Freeh was very clear in disavowing any interest in covering such information:

[Call setup information] does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent to include, however, with reference to this term, to acquire anything that could properly be called 'tracking' information.

Digital Telephony Hearings, supra note 9, at 29.

- - - - -End Footnotes- - - - -

(2) Packet switching. In a decision that has potentially far-reaching implications for the future of telephony, the Internet and government surveillance, the proposed CALEA implementation standard issued in July 1997 would allow telecommunications companies using "packet switching" n172 to provide the full content of customer communications to the government even when the government is only authorized to intercept addressing or signaling data. n173 Despite indications that it is feasible to provide signaling information separate from the content in a packet switching environment, the proposed standard would allow companies to deliver the entire packet data stream, including call content, when law enforcement is entitled to receive

only dialing or signaling information under a pen register order. Such orders are issued without probable cause and without the discretionary review accorded to full call content interceptions. The proposed CALEA standard relies on law enforcement to sort out the addressing information from the content, keeping the focus on the latter. This approach, were it followed, could totally obliterate the distinction between call content and signaling information that was a core assumption of ECPA and of CALEA itself. It also would violate section 103(a)(4) of CALEA, which requires the telecommunications industry to protect communications not authorized to be intercepted.

-Footnotes-

n172. In the future, telecommunications systems will rely increasingly on "packet switching" protocols similar to those used on the Internet. This development has potentially profound implications for government surveillance. In a packet switching system, communications are broken up into individual packets, each of which contains a segment of the communication plus addressing information that gets the packets to their intended destination, where they are reassembled. Previously utilized primarily on the Internet for electronic communications, this technology offers substantial advantages in the voice environment as well, and telecommunications companies are beginning to incorporate it in their systems. See OTA Electronic Surveillance Report, supra note 108, at 57-61.

n173. SP 3580-A, supra note 148, at 22-25.

-End Footnotes-

In the old analog systems, law enforcement agencies authorized to receive signaling information were provided with access to the target's entire line, including content. n174 With subsequent developments in technology, the signaling data was carried on a channel separate from the call content. In this respect, technology itself enhanced privacy, creating an environment in which a law enforcement agency conducting a pen register could receive only information it was entitled to receive. Absent CALEA, packet switching might have reversed the privacy enhancement. However, CALEA imposed on the industry an affirmative obligation to protect privacy. Yet, the proposed industry standard initially failed to ensure that law enforcement agencies receive only the information appropriate to the level of authorization in hand.

-Footnotes-

n174. See *Ellis v. State*, 256 Ga. 751, 753, 353 S.E.2d 19, 21 (1987).

-End Footnotes-

Another capability sought by the FBI, but rejected by industry as of November 1997, was the ability to monitor all conversations during a conference call initiated by a targeted facility, even if the targeted facility is on hold or has hung up from the call. n175 It is [*99] questionable whether law enforcement has authority under the particularity requirement of the Fourth Amendment and Title III to intercept communications involving only non-targeted facilities just because a targeted facility initiated a conference call.

-Footnotes-

n175. The matter arises as follows: A is the intercept subject. A sets up a conference call with B and C using the conference call capability provided by A's service provider. Then A puts B and C on hold (or hangs up entirely) and calls D. The FBI is seeking the delivery of both A's conversation with D and the conversation between B and C. It is not clear that there is legal authority to intercept the ongoing conversation between B and C after A has hung up. Title III, embodying the Fourth Amendment standard of particularity, requires the specification in the order of the telephone facility to be tapped and the particular conversations to be seized. The Supreme Court has held that conversations between unknown individuals using a specified telephone line could be lawfully intercepted under Title III. See *United States v. Kahn*, 415 U.S. 143 (1973). Lower courts have upheld the roving tap authority so long as it is limited to the interception only of conversations of named subjects. See *United States v. Ferrara*, 771 F. Supp. 1266, 1318 (D. Mass. 1991); *United States v. Silberman*, 732 F. Supp. 1057, 1062 (S.D. Cal. 1990). No court has held that there is authority to intercept the communications of unknown persons using unspecified facilities while the named target is on another monitored call.

- - - - -End Footnotes- - - - -

A number of the enhancements sought by the FBI were related to the Bureau's attempts to exploit transactional data. In legislative terms, the FBI tried to force more information into the definition of the CALEA term "call-identifying information." The plain language of CALEA and the legislative history indicate that "call-identifying information" means the numbers dialed by a subscriber to direct a communication, or other signaling information that serves the same call routing purpose as the dialed digits. This includes the switch-based information equivalent to a seven or ten digit phone number that directs a call when a voice dialing or speed dialing feature is used. n176 The term likely includes information indicating that the party under surveillance has terminated a call by hanging up. However, the FBI argued that this term includes much more. For instance, at various points in the CALEA implementation process, the FBI argued that carriers must build in the capability to provide not only location-related information on wireless phone users, but "location-related updates during [redacted]." The Bureau also asked for detailed "call progress" tones relating to [redacted] the target of the investigation and persons with whom the target is communicating, and messages during three-way calls that would indicate when a party, who is not the target of the surveillance, drops off a three-way call. Further, the FBI sought "voice message waiting" tones to notify the government when a surveillance target has a voice mail waiting and feature status messages that would notify the government in real [*100] time when a surveillance target changes his or her mix of service features. n177

- - - - -Footnotes- - - - -

n176. H.R. Rep. No. 103-827, at 21 (1994).

n177. ESI Document, supra note 144, at 36 (party disconnect, party hold, and party join messages), 34 (message waiting indicator), 32 (feature status message).

- - - - -End Footnotes- - - - -

D. The Role of Congress and the FCC in Ensuring Balanced Implementation of CALEA

B... Congress and the Federal Communications Commission (FCC) have oversight responsibility to ensure that CALEA is properly implemented in a way that preserves the crucial balance between privacy and law enforcement powers.

CALEA requires the FBI to obtain annual appropriations for implementing the law. n178 This has allowed the House and Senate Appropriations Committees to examine the issues posed by implementation and to withhold funds until they are satisfied that implementation is proceeding appropriately. In 1995, the first year after CALEA was enacted, Congress declined to appropriate any funds for implementation. n179 In 1996, Congress established a CALEA Compliance Fund but blocked the FBI from expending any funds until it had submitted a detailed implementation plan. n180 In 1997, after reviewing the implementation plan, both Houses expressed concern about the lack of priority in the FBI's plan. The Senate Appropriations Committee declined the Administration's request for \$ 100,000,000. n181 Instead, the Committee directed the FBI to create a working group with the purpose of creating "a more rational, reasonable, and cost-effective CALEA implementation plan." n182 The Committee recommended that no funds be expended for CALEA implementation until the working group provided a plan satisfactory to the Committee. n183 The House-Senate conference committee on the fiscal 1998 appropriation for the Department of Justice came to a somewhat different resolution. The conference agreement, which passed the Congress and was signed into law, included no additional funding for CALEA implementation, but the report noted that there had been recent discussions between the Committees on Appropriations, [*101] the Justice Department and representatives of the telecommunications industry. n184 As a result of these discussions, the conference report stated, an agreement had been reached, which included a commitment by industry and law enforcement to provide to the Committees on January 4, 1997 cost estimates for the deployment of "the solution," along with a timetable for deployment and signed agreements from two carriers or equipment manufacturers (presumably to begin development of the solution). n185

-Footnotes-

n178. See Pub. L. No. 103-414, 110; H.R. Rep. No. 103-827, at 19 (1994).

n179. See Pub. L. No. 104-99.

n180. H.R. Rep. 104-863 (1996), printed in Cong. Rec. H1164, H11646 and H11649-50 (1996).

n181. S. Rep. No. 105-48, at 23 (1994).

n182. Id.

n183. Id.

n184. 143 Cong. Rec. H10836 (1997).

n185. Id.

-End Footnotes-

The FCC has ample jurisdiction to ensure that CALEA implementation protects privacy. The most important source of the FCC's jurisdiction is section 107 of CALEA, which authorizes the Commission to intervene to establish an implementation standard if the industry standard-setting process fails to produce an acceptable standard. n186 In that event, the FCC is required to ensure that the standard protects the privacy and security of communications not authorized to be intercepted and achieves other specified public policy goals, including promotion of technology innovation. n187 Any party, including public interest groups, may seek a proceeding under section 107 to challenge CALEA implementation. Also, section 105 of CALEA requires that carriers ensure that any interception within their switching premises be activated only in compliance with a court order and with the affirmative intervention of an individual officer or employee of the carrier. These provisions give the FCC ample authority to reject elements of the FBI-industry implementation standard that go beyond preserving the status quo and that do not adequately protect privacy. Attention also needs to be given to law enforcement compliance with the new language in the pen register and trap and trace section, requiring the use of reasonably available technology that limits pen registers and trap and trace devices to the collection of "dialing and signaling information used in call processing." n188

- - - - -Footnotes- - - - -

n186. Section 107 of CALEA states:

If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a Government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards that... (2) protect the privacy and security of communications not authorized to be intercepted.

47 U.S.C. 1006.

n187. CALEA, 107(b)(1)-(5) (codified at 47 U.S.C. 1006 (b)(1)-(5)).

n188. 18 U.S.C. 3121(c) (1996).

- - - - -End Footnotes- - - - -

[*102]

E. CALEA as an Exercise in Control and Accountability

CALEA imposed on the nation's telecommunications systems an unprecedented new obligation: to design their systems and services with the objective (along with all their other objectives related to provision of quality service) of ensuring the government's ability to carry out electronic surveillance. It was the judgment of Congress that wiretapping was a law enforcement capability worth preserving. And Congress had before it the acknowledgment of industry

representatives that, unless action was legislatively forced, the electronic surveillance capability might be lost or substantially diminished as a result of technological development. n189 However, Congress fully recognized the dangers to privacy and technological innovation inherent in what it was mandating. Therefore, Congress wove throughout CALEA a series of limitations, and it established a series of checks and balances, lodging in a number of entities authority to influence or control the implementation of the law.

-Footnotes-

n189. H.R. Rep. No. 103-827, pt. 1, 15-16 (1994).

-End Footnotes-

Thus, CALEA spelled out four capability requirements. n190 These four requirements, while phrased in general terms, are nonetheless exclusive; anything that law enforcement would want to require under CALEA has to fit under one of these four requirements or it cannot be mandated. Further, Congress specifically excluded certain capabilities. It specified that carriers have no obligation to ensure the ability to unscramble encrypted communications when the user controls the encryption keys. n191 It specified that a given carrier has no responsibility to continue monitoring when a target using cellular roaming moves out of the carrier's service area and into the service area of another carrier. n192 The legislation denied to law enforcement any authority to dictate system design. n193 Instead, the legislation defers to industry to establish standards. n194 Any publicly available standard adopted in good faith to implement the requirements of the law constitutes a safe harbor. Companies are deemed in compliance with the act if they comply with the industry standard. n195 Law enforcement cannot unilaterally declare a standard deficient. If law enforcement [*103] is not satisfied with the industry standard, it must petition the FCC to adopt a different standard, and the FCC's latitude is limited by a specified set of criteria that must guide the development of a standard. n196

-Footnotes-

n190. CALEA, 103(a)(1)-(4) (codified at 47 U.S.C. 1002(a)(1)-(4)).

n191. Id. at 103(b)(3) (codified at 47 U.S.C. 1002(b)(3)).

n192. Id. at 103(d) (codified at 47 U.S.C. 1002(d)).

n193. Id. at 103(b)(1) (codified at 47 U.S.C. 1002(b)(1)).

n194. Id. at 107(a) (codified at 47 U.S.C. 1006(a)).

n195. CALEA, 107(a) (codified at 47 U.S.C. 1006(a)).

n196. CALEA, 107(b) (codified at 47 U.S.C. 1006(b)).

-End Footnotes-

The concept of "reasonableness" appears throughout the legislation. Carriers are obligated to make available only such call-identifying data as is "reasonably available." n197 The FCC may grant an extension of time for compliance if compliance within the specified period is not "reasonably

achievable." n198 A court can order compliance only if alternative technologies or facilities of another carrier are not "reasonably available" to law enforcement for implementing the interception and only if compliance is "reasonably achievable." n199 Carriers are not required to bear the costs of retrofitting equipment installed before January 1, 1995 if compliance is "not reasonably achievable." n200

-----Footnotes-----

n197. Id. at 103(a)(2) (codified at 47 U.S.C. 1002 (a)(2)).

n198. Id. at 107(c) (codified at 47 U.S.C. 1006(c)).

n199. Id. at 108(a) (codified at 47 U.S.C. 1007(a)).

n200. Id. at 109(b)(2) (codified at 47 U.S.C. 1008(b)(2)).

-----End Footnotes-----

Congress also included in CALEA mechanisms of public accountability. Capacity requirements must be adopted only after a public notice and comment proceeding in the Federal Register. n201 Technical standards for implementing the capability requirements have to be "publicly available." n202 Funding is subject to the annual appropriations process, with hearings, reports, and enacted laws. The Attorney General is required to issue periodic reports on implementation. n203

-----Footnotes-----

n201. CALEA, 104 (codified at 47 U.S.C. 1003).

n202. Id. at 107(a)(2) (codified at 47 U.S.C. 1006(a)(2)).

n203. Id. at 112 (codified at 47 U.S.C. 1010).

-----End Footnotes-----

As a series of checks and balances, CALEA placed authority over implementation in a number of hands. Thus, industry bodies develop the standards. Upon the petition of industry, law enforcement or any other person, the FCC can develop a superseding standard. The FCC was also granted the authority to issue extensions of the compliance deadline, and to determine that compliance is not reasonably achievable with respect to a certain service or carrier. The courts have jurisdiction over compliance proceedings. n204 Congress has control through its appropriations committees, which must annually appropriate funds for compliance and therefore can use the power of the purse to control how [*104] the legislation is being implemented. n205 The Judiciary Committees and the Commerce Committees, as the authorizing committees, can always revisit the legislation and amend it as circumstances change and in light of experience.

-----Footnotes-----

n204. Id. at 108(a) (codified at 47 U.S.C. 1007(a)).

n205. CALEA, 110 (codified at 47 U.S.C. 1009).

-----End Footnotes-----

the CALEA legislation to work in a balanced fashion, the limitations and reasonableness provisions written into law by Congress must be invoked and the entities with responsibility for overseeing the implementation of the statute must choose to exercise their authority to preserve the intended balance. The FBI has substantial resources and the politically powerful anti-crime rhetoric at its disposal, and it has the ability to mobilize state and local law enforcement to promote its position. Thus, the FBI will dominate the implementation process unless the other government institutions exercise the authority granted them under the statute to promote the counterbalancing values of privacy and innovation. In this sense, CALEA is merely one more manifestation of the on-going efforts in our democratic society to regulate the police and national security powers of the government. Congress, deeming it necessary to preserve an electronic surveillance authority, can legislate limits and controls, but those limits must be enforced and the controls must be exercised by the executive and regulatory agencies, future Congresses, and the courts.

VI. Realizing the Privacy-Enhancing Potential of Encryption Technology

Illegal electronic intrusion into computer networks is a rapidly escalating crime problem. White collar criminals, economic espionage agents, organized crime groups, foreign intelligence agents, and terrorist groups have been identified as "electronic intruders" responsible for penetrations of American computer networks. It is estimated that the Pentagon's computers are subject to hackers' attempts 250,000 times a year. The United States Government relies upon the National Information Infrastructure (NII) for the efficient, uninterrupted flow of electronic information for air traffic control, military communications, energy distribution, public safety, and other essential government programs and services. Intelligence and industry forecasts indicate the United States is just beginning to realize the potentially damaging effects and extent of the computer crime problem. n206

-----Footnotes-----

n206. FBI, U.S. Dept. of Justice, FY 1998 Authorization and Budget Request for the Congress, at A-3 (1997).

-----End Footnotes-----

[*105]

On balance, the advantages of more widespread use of cryptography outweigh the disadvantages. n207

-----Footnotes-----

n207. NRC Report, supra note 3, at 300.

-----End Footnotes-----

Newer communications media are inherently insecure. n208 Wireless telephones have great advantages in convenience compared with wireline counterparts, yet, since wireless phones transmit over the airwaves, eavesdropping is easier not only for curious neighbors but also for burglars identifying potential targets and industrial spies stealing trade secrets. n209 Similarly, decentralized computer networks such as the Internet have low barriers to entry, are much less expensive, are more robust and can be used to accomplish a far greater variety of tasks than the proprietary networks of the past, but, again, at the expense of intrinsic security. The vulnerabilities of the national and global information infrastructures have been recognized not only by the FBI, but also by the Defense Science Board Task Force on Information Warfare-Defense n210 and by the President's Commission on Critical Infrastructure Protection. n211 The losses to date from inadequate system security are enormous. In one series of transactions in 1994, an international group of criminals penetrated Citicorp's computerized electronic transfer system and moved about \$ 12 million from legitimate customer accounts into their own accounts in banks around the world. n212 In 1996, after a comprehensive study, the National Research Council concluded, "Of all the information vulnerabilities facing U.S. companies internationally, electronic vulnerabilities appear to be the most significant." n213

-----Footnotes-----

n208. Hal Abelson et al., The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption, at 5 (1997).

n209. See Cellular Privacy Hearing, supra note 2.

n210. Report of the Defense Science Board Task Force on Information Warfare-Defense (Nov. 1996) (last modified June 29, 1997) <<http://www.jya.com/iwd.htm>>. The Task Force recommended spending \$ 3 billion over the next five years hardening the nation's telecommunications infrastructure against attack, noting that the Defense Information Infrastructure is largely dependent upon the commercial telecommunications infrastructure.

n211. President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructure (Nov. 1997) available at <<http://www.pccip.gov/report/index.html>>.

n212. See NRC Report, supra note 3, at 23.

n213. Id. at 31.

-----End Footnotes-----

Given these inherent vulnerabilities, widespread use of encryption to protect communications and stored data is essential to prevent fraud and other forms of crime in the digital age. At the same time, encryption poses challenges to law enforcement and [*106] national security agencies, which have raised the specter of criminal suspects' undecipherable stored information or voice communications. This has led to a vigorous legislative debate over control of encryption technology. n214

-----Footnotes-----

4. Id. at 31.

-----End Footnotes-----

In some ways, the encryption debate has been a conflict between two competing models of security, one in which private individuals, businesses and governments choose from a variety of encryption options to protect their security, and another wherein the federal government assumes the primary responsibility for protecting personal and business as well as governmental security through government-promoted weaknesses in encryption technology. n215 While there are law enforcement equities on both sides of the encryption issue, the centralized model of security based on government-controlled encryption weaknesses is incompatible with certain defining characteristics of the digital communications revolution: decentralization, competition, globalization, and the dynamics of decreasing cost and increasing computing power that have put more control and more choices in the hands of end users.

-----Footnotes-----

n215. See Abelson et al., supra note 208, at 6-7.

-----End Footnotes-----

The Executive Branch's various efforts to impose a centralized model of security on a decentralized medium have delayed full realization of the Internet's economic, personal and democratizing potential. They have also hurt the competitiveness of American computer companies by prohibiting export abroad, thereby inhibiting in the U.S. the use of strong encryption that is already available overseas. n216 At the same time, given the already widespread proliferation of user-controlled encryption technology, the centralized model cannot offer assurances of achieving the desired law enforcement access. Strong non-escrowed encryption is and will continue to be available to those who want it. There are currently hundreds of encryption products available worldwide. The National Research Council to conclude that, on balance, the security-enhancing, crime-preventing benefits of encryption outweigh the impediments to law enforcement. n217

-----Footnotes-----

n216. It has also been argued that there is a First Amendment right to use and export encryption. See Bernstein v. Department of State, 945 F. Supp. 1279 (N.D. Cal. 1996).

n217. NRC Report, supra note 3, at 300.

-----End Footnotes-----

Globalization is a key factor, and the global market has rejected all government proposals to control encryption technology. U.S. proposals in 1993 for government agencies to serve as key escrow [*107] agents were immediately rejected by business and individual users as involving an unacceptable level of vulnerability. n218 More recent approaches that depend

upon government licensing or "registration" of escrow agents or other forms of government control of decryption mechanisms (including proposals to require key recovery features as a condition of receiving public key certificates) are also not relieving market acceptance. n219 The type of ubiquitous, near-instantaneous key escrow, key recovery, or key management "infrastructure" sought by the U.S. government is so complex, so vulnerable, so expensive and/or so cumbersome - so fundamentally at odds with user needs - that it will not be accepted by users. n220

-----Footnotes-----

n218. John Markoff, Computer Code Plan Challenged, N.Y. Times, May 29, 1993; John Markoff, Panel Sees Flaws in Plan for Encoding, N.Y. Times, June 5, 1993; John Schwartz, U.S. Data Decoding Plan Delayed, Wash. Post, June 8, 1993, at A12.

n219. Edmund L. Andrews, U.S. Restrictions on Exports Aid German Software Maker, N.Y. Times, Apr. 7, 1997, at D1.

n220. See Abelson et al., supra note 208.

-----End Footnotes-----

Yet the market alone will not address all of the privacy issues posed by encryption. While it seems clear that most businesses and individuals will not trust the government or government-dictated private structures to hold their keys, it also seems clear that under some encryption applications, particularly those involving stored data, some users are interested in securing a means to recover their encrypted data if they lose their own key. (There is less incentive for development of key escrow for transmissions.) Market-based efforts to address this problem - responses to user needs - are resulting in a range of key escrow, key recovery, or "trusted third party" systems for decryption assistance. n221 These are quite different from the systems proposed by the Administration under its legislative proposal, which is voluntary in name only. n222 These user-driven, user-controlled data-recovery or key escrow arrangements will offer law enforcement an opportunity to satisfy many of its basic access needs for stored data. n223

-----Footnotes-----

n221. See id.

n222. Id.

n223. In many cases (e.g., suspects communicating with their banks or engaging in credit card transactions or other on-line commercial transactions), there will be plaintext of messages and data readily available to the government by subpoena or other legal process.

-----End Footnotes-----

As the market develops key recovery arrangements, government agencies will be seeking access to those keys for law enforcement and national security purposes, to decrypt seized files and [*108] communications intercepted under the wiretap laws. Government efforts to access stored keys will pose obvious

privacy concerns. Given the centrality of encryption to privacy and security in the digital age, there is a strong argument that escrowed encryption keys and key recovery assistance should be entitled to greater protection than that traditionally accorded to so-called "third party records." In the past, as noted above, in Section IV, the courts have accorded little Fourth Amendment protection to business records like checks or credit card records created in the course of commercial transactions and knowingly revealed to banks and other third parties. n224 The Fourth Amendment, however, may have stronger application to especially sensitive information such as a decryption key entrusted to a third party under an escrow arrangement. n225 Disclosure of keys, even escrowed keys, also raises serious questions under the Fifth Amendment's protection against compelled self incrimination. n226

-----Footnotes-----

n224. United States v. Miller, 425 U.S. 435 (1976); Fisher v. United States, 425 U.S. 391 (1976).

n225. The compelled disclosure of decryption information poses concerns quite different from those normally applied to business records under Miller and Fisher. Current Fourth Amendment jurisprudence suggests that the government cannot always use a mere subpoena to compel even from a third party production of a person's private, personal documents. Fisher, 425 U.S. at 401 n. 7; 1 Sara S. Beale et al., Grand Jury Law and Practice, 6.27 (1986 & 1996 Cum. Supp.).

n226. Generally, the courts have held that a voluntarily created document does not contain compelled testimonial evidence. Almost all these cases, however, have arisen in the context of business records. The leading case, Fisher v. United States, supra, involved a subpoena of accountants' workpapers relating to two taxpayers, which were in the possession of the taxpayers' attorney. The Fisher Court itself recognized that there may be some category of private papers that are protected under the privilege against self-incrimination. Fisher, 425 U.S. at 414. The federal Circuit Courts of Appeals are split. Two federal Appeals Courts have held that the Fifth Amendment bars compelled disclosure of private, non-business papers. United States v. [redacted], 636 F.2d 1028 (5th Cir. 1981), cert. denied, 454 U.S. 862 (1981); In re [redacted] Jury Proceedings, 632 F.2d 1033 (3d Cir. 1980).

-----End Footnotes-----

Encryption will play a central enabling role in the protection of privacy in the digital age. Government attempts to access keys or decryption assistance will raise important privacy interests. Reliance on the courts to sort out the issues will produce a possibly long period of uncertainty and conflicting decisions. Legislative action setting clear privacy standards for government access to keys and decryption assistance held by second or third parties would be far preferable. Such legislation should include standards that prohibit escrow agents from providing keys or decrypt [*109] tion assistance except in conformity with a court order issued upon a finding of probable cause and a showing that there is no feasible alternative of obtaining the plaintext, and should require minimization in the use of the key or assistance. n227

-----Footnotes-----

n227. Sen. Patrick J. Leahy (D-VT) introduced legislation in the 105th Congress, S. 376, with elements of such a privacy protection scheme.

- - - - -End Footnotes- - - - -

II. Protecting Wireless Communications

In the network of networks that comprises the telecommunications "system" of today and the future, it is no longer appropriate to look at wireless telephone systems as distinct from wireline systems or to look at the telephone system as separate from the Internet. The increasing use of wireless communications services, the seamless integration of wireless and wireline networks, and the importance of wireless data links heighten the urgency of ensuring the privacy and security of wireless communications. In this context of a global communications network increasingly dependent on wireless links, it is a serious invasion of privacy to eavesdrop on wireless telephone conversations. n228 Wireless eavesdroppers are invading the privacy not only of the person who is using a wireless phone, but also of anybody else who is in the conversation using an ordinary landline telephone. As wireless telephones become more ubiquitous, scanning threatens the privacy of all telephone users. n229

- - - - -Footnotes- - - - -

n228. Cellular Privacy Hearing, supra note 2, at 10-11 (testimony of Jerry Berman).

n229. Id.

- - - - -End Footnotes- - - - -

Encryption will play an essential role here too, for securing over-the-air links. But it is clear that there is a need for legislative improvements clarifying both the prohibitions against unauthorized private interception and the legal standards for governmental access to wireless transmissions.

Location information. As noted already, wireless telephone systems are improving the capability to provide more refined location information on wireless phone users. Nonconsensual government monitoring of location through a wireless phone implicates privacy interests. n230 Since wireless telephones are regularly carried [*110] into places where a person has a reasonable expectation of privacy, Congress should clarify the law by requiring a warrant based on a showing of probable cause for nonconsensual governmental access to real-time wireless telephone location information.

- - - - -Footnotes- - - - -

n230. In *United States v. Karo*, the Supreme Court held that the monitoring of a beeper in a private location is a search subject to the Fourth Amendment warrant requirement. 468 U.S. 705, 706 (1984). The Court distinguished this from the use of a beeper to follow an object being transported on the public roads, or to monitor the general vicinity of an object, both of which had been held not to implicate the Fourth Amendment in *United States v. Knotts*, 460 U.S. 276 (1983). *Karo*, 468 U.S. 705, 714-716. Obviously, wireless phones are carried by their users into places where there is a legitimate expectation of privacy. Wireless phone location tracking through the facilities of service providers

is becoming more precise, as a result of the E-911 requirements imposed by the FCC E-911 Order, and as a result of technical developments that are producing smaller and smaller cell sites and cell sectors. FCC E-911 Order, *supra* note 85. If anything, monitoring the location of wireless phones is more intrusive than that of a beeper. The beeper cases usually involve the attachment of the beeper to an object (often contraband or precursor chemicals for illegal drug manufacture). Unlike drums of precursor chemicals, cellular phones are often directly associated with an individual user. They implicate movements of the person going about his or her daily life and entering a variety of locations (homes, offices) where there is a legitimate expectation of privacy. The ongoing nature of such monitoring (as opposed to the tracking of a barrel of precursor chemicals from the manufacturer to the clandestine laboratory in the typical beeper case) raises much more serious privacy interests. These interests merit full Fourth Amendment protection.

- - - - -End Footnotes- - - - -

Wireless data transfers. At a time when wireless local area networks are proliferating and when wireless data transmissions could be used for everything from proprietary data to medical records, it is not clear that wireless data transfers are protected to the same extent as wireless voice communications. The status of legal protection for wireless data transfers has a confused history, leaving it unclear whether they are currently protected by ECPA. An industry and privacy task force concluded in 1991 that wireless transfers of data might not be covered by ECPA, and recommended that coverage be extended. n231 In 1994, in CALEA and with the support of the Administration, Congress passed a provision making it clear that the privacy of wireless data transfers was protected by ECPA. n232 But less than two years later, in the anti-terrorism act of 1996, Congress repealed the provision on the basis of the Justice Department's claim that the 1994 amendment was inappropriately overbroad. n233

- - - - -Footnotes- - - - -

n231. See Digital Telephony Hearings, *supra* note 9, at 179, 183 (Final Report of the Privacy and Technology Task Force Submitted to Senator Patrick J. Leahy).

n232. See Pub. L. No. 103-414, 203, 108 Stat. at 4291 (1994) (amending 18 U.S.C. § 2510(16)).

n233. Pub. L. No. 104-132, 731 (1996). The repeal came at the behest of the Justice Department, which argued that the privacy provision was inappropriately overbroad, and included ham radio and CB radio broadcasts, which should not be privacy-protected. The Justice Department, reversing the Administration's earlier provision, argued that wireless data transfers were already protected. Rather than propose narrower language to make that clear, the Administration successfully argued for repeal of the entire provision. In the context of the many issues in the terrorism bill, this one received little attention.

- - - - -End Footnotes- - - - -

[*111]

This confusion should be resolved by appropriate legislative language extending the privacy protections of ECPA unambiguously to wireless data transfers.

Interception devices. ECPA made it a crime to manufacture, sell, assemble, possess or advertise any device that is "primarily useful" for the interception of wireless telephone conversations. n234 Unfortunately, the effectiveness of this provision is quite limited, since it is difficult to prove that a device capable of intercepting cellular and a range of other frequencies is "primarily useful" for prohibited interceptions. Congress should delete the word "primarily," at least as it affects manufacture, sale, assembly, and advertisement.

-----Footnotes-----

n234. See 18 U.S.C. 2512 (1996).

-----End Footnotes-----

The manufacture and import of scanners equipped or readily alterable to receive transmissions in frequencies assigned to the "domestic cellular radio telecommunications service" are prohibited under section 302(d) of the Communications Act. n235 However, since the enactment of this provision, a new category of services called "commercial mobile radio services" has been created, into which cellular, as well as additional mobile services at different frequency ranges, such as personal communications systems (PCS), have been added. The law does not appear to prohibit manufacture and import of devices equipped to scan these frequencies. Congress should extend the section 302 prohibition to the parts of the spectrum used for PCS and other wireless telephone communications.

-----Footnotes-----

n235. 47 U.S.C. 302(a)(d) (1996).

-----End Footnotes-----

VIII. Strengthening the Wiretap Laws to Reestablish the Principles of Katz and Berger

The balance among the interests of law enforcement, privacy and technological innovation has come under challenge in recent years. Steadily growing numbers of wiretaps, longer and longer surveillances intercepting more and more communications suggest that the wiretapping laws are not working as originally intended to constrain the use of this highly intrusive technique. These developments point to the need for amendments to the law to reestablish the balance Congress originally sought. Until such corrective amendments are enacted, it would be premature to consider proposals to further expand the scope of, or weaken the privacy protection standards in, the wiretap laws.

Unfortunately, the focus of the legislative debate recently has been in the opposite direction, on proposals to give the government greater latitude in wiretapping. As noted above in Section VII, the Justice Department sought and obtained repeal of one of the privacy protections that were adopted in CALEA. Further, the President sought in his terrorism legislation a series of other changes in the wiretap laws that would have weakened the sanctions against illegal government wiretapping; weakened the standards for so-called "roving taps;" and expanded the availability of warrantless taps in "emergency"

situations. n236 While these other changes were ultimately rejected, they were considered and debated without attention to counterbalancing proposals to enhance privacy.

-----Footnotes-----

n236. Omnibus Counterterrorism Act of 1995, H.R. 896 (1995); S. 390 (1995). See also Comprehensive Antiterrorism Act of 1995, H.R. 1710 (1995) (Republican terrorism bill).

-----End Footnotes-----

The Clinton Administration has continued to support these and other changes in the wiretap laws. In July 1996, the Department of Justice submitted to Congress a report recommending eight amendments to the federal electronic surveillance laws, including the change in the statute's exclusionary rule, the loosening of the standard for "roving taps," and additional authority for emergency wiretaps without judicial approval. n237 The report stated that "several other proposed amendments are under consideration by the Department, ... [which] are expected to be submitted to Congress at a later time." n238

-----Footnotes-----

n237. See July 1996 Electronic Surveillance Report to Congress, *supra* note 6.

n238. *Id.* Significantly, the Justice Department report was able to identify only one revision to the wiretap laws that would have enabled law enforcement authorities to better fulfill their responsibilities. This was the addition of an additional predicate offense for the use of wiretapping, namely, 18 U.S.C. 842, involving manufacturing, dealing in, and importing explosive materials without a license and the unlawful distribution of explosive materials.

-----End Footnotes-----

By far, the most dangerous change the Administration proposed was an amendment to Title III to allow courts to receive evidence obtained in violation of the wiretap law. When Title III was adopted, Congress included a statutory exclusion rule, calling it "an integral part of the system of limitations designed to protect privacy." n239 The Administration proposal, although sometimes described as a good faith exception, would require a person to [*113] prove "bad faith" on the part of the government, before evidence will be excluded for violation of the law - an almost impossible undertaking. The Administration's 1995 proposal was not limited to situations where law enforcement officers relied on a technically defective warrant. n240 The Supreme Court has already held that the statutory suppression or exclusion rule in Title III is not to be applied to technical violations. n241 The Administration proposal would apply to all provisions of the wiretap law, including those governing the conduct of the government after the warrant is issued. Thus, it would remove the only real incentive against violating such central protections as the minimization and evidence preservation rules. The Administration argued that the proposed change would merely apply to wiretaps the same standard applicable to other searches. However, the constitutional presupposition of Title III is that special, heightened standards are necessary for electronic surveillance because of its unique nature. n242

-----Footnotes-----

n239. S. Rep. No. 90-1097, at 96 (1968).

. S. 390, at 105 (1995) (Omnibus Counterterrorism Act of 1995).

n241. United States v. Giordano, 416 U.S. 505, 527-28 (1974) ("We think Congress intended to require suppression where there is failure to satisfy any of those statutory requirements that directly and substantially implement [the intended limitations on the use of wiretapping]" (emphasis added)).

n242. S. Rep. No. 90-1097, at 96 (1968).

-----End Footnotes-----

If amendments to the wiretap laws are to be considered, then it must be in the context that gives equal weight to an examination of issues from a privacy perspective. It should be clear from the discussion in Section II (B) that amendments are necessary to repair the damage done by judicial interpretation. Specifically, it is time to strengthen the minimization rule and to clarify the requirement that law enforcement exhaust other techniques before seeking an interception order. Other changes are necessary as well:

Transactional data. Advanced signaling systems for voice communications have blurred the distinction between call identifying information and call content. Currently, the standards for governmental access to signaling data under what are known as "pen registers" and "trap and trace devices" require a court order, but the statute puts the judge in a purely ministerial role: the sole function of the judge is to determine whether the signature of an Assistant United States Attorney is on the application. n243 One improvement would be an amendment requiring that the judge exercise discretion and only approve the request upon finding, [*114] based on a showing by the government, that the information sought is relevant and material to an ongoing criminal investigation. As argued in Section VII, above, one type of transactional data, namely real-time location information generated in wireless telephone systems, implicates such serious privacy interests that Congress should clarify the law by requiring a warrant on a showing of probable cause for nonconsensual governmental access to such information when obtained on a real-time, tracking basis. In light of the growing significance of transactional and signaling data, it is time for Congress to examine more generally the implications of government access to and analysis of all forms of such information for subscriber profiling purposes.

-----Footnotes-----

n243. See 18 U.S.C. 3123(a) (1996).

-----End Footnotes-----

Roving wiretaps. The Justice Department has proposed loosening the standard for so-called roving or multi-point wiretaps. n244 Roving taps (taps placed on a phone line other than the line subscribed to by the target of a surveillance order) are considered especially sensitive because they often entail tapping the phone of someone who is not the subject of an investigation and not suspected of any involvement in criminal conduct. n245 The Justice Department argues that the current statute requires the government to show the subjective intent of the

subject to evade interception. n246 The Department argues that it should be enough that the subject's actions have the objective result of thwarting interception. n247 If Congress changes the standard for roving taps, it should add to the law an explicit prohibition against interception of the conversations of innocent third parties, so that such conversations would be outside the scope of the warrant. While this conforms to stated Justice Department policy and the few lower court decisions, n248 it would be desirable to write the principle into the Title III statute.

-----Footnotes-----

n244. See 18 U.S.C. 2518(11) (1996); S. 390, at 108 (1995).

n245. See e.g. United States v. Bianco, 998 F.2d 1112, 1122-24 (1st Cir. 1993), cert. denied, 114 S. Ct. 1644 (1994). See generally, Michael Goldsmith, Eavesdropping Reform: The Legality of Roving Surveillance, 1987 U. Ill. L. Rev. 401 (1987).

n246. See July 1996 Electronic Surveillance Report to Congress, supra note 6, at 33-34.

n247. See id. See also H.R. Rep. 104-383 (1995) (Comprehensive Antiterrorism Act) (citing "today's rapidly changing telecommunications technology" and the widespread use of "cellular telephones, pagers, portable fax machines and portable computers" as justification for the roving tap changes).

n248. See United States v. Ferrara, 771 F. Supp. 1266, 1318 (D. Mass. 1991); United States v. Silberman, 732 F. Supp. 1057, 1062 (S. D. Cal. 1990).

-----End Footnotes-----

[*115]

Emergency wiretaps. Title III allows the use of wiretapping without court approval in emergency situations involving immediate danger of death or serious physical injury, threats to the national security, or organized crime. In such cases, an application for a court order must be filed within forty-eight hours. The Administration has recommended expanding this emergency authority to include terrorism cases that do not involve an immediate danger of injury or threat to the national security. n250

-----Footnotes-----

n249. 18 U.S.C. 2518(7) (1996).

n250. See S. 390, at 107 (1995).

-----End Footnotes-----

More appropriate than the Administration's proposed change would be a careful reexamination of the Title III emergency exception itself. The emergency exception was enacted in 1968. Now, given the pervasiveness of faxes, wireless telephones, and e-mail, it is hard to understand why it would ever be impossible or even difficult to reach a federal judge to obtain prior approval for electronic surveillance. It should be noted that in 1977 the Federal Rules of Criminal Procedure were amended to allow for telephonic submission of search

warrant applications and affidavits in emergency situations, with procedures for contemporaneous recording of the oral testimony supporting probable cause. n251 This seems to be a far more appropriate model for updating the emergency tap authority of Title III. n252

-----Footnotes-----

n251. Fed. R. Crim. P. 41(c)(2) (1997).

n252. In addition, it would be appropriate to update the emergency procedures under FISA, 50 U.S.C. 1805(e), written in 1979, which allow emergency taps for twenty-four hours.

-----End Footnotes-----

Limiting use of FISA in criminal cases. In most FISA cases, since the target is never notified of the existence of the surveillance, there is never an opportunity for after-the-fact adversarial review of the legality of the taps. n253 Even if there is a criminal investigation and notice is provided, the adversarial hearing is inadequate because the target is not allowed to see the affidavit that provided the basis for the order. The increasing use of FISA intercepts in criminal cases suggests that FISA is turning out to be a bigger than expected exception to ordinary wiretap procedures. n254 In espionage cases involving U.S. persons, long after it is clear that the subject is suspected of engaging in espionage, and [*116] long after there is adequate basis to open a criminal case and obtain a wiretap order under Title III, the FBI continues to proceed under a FISA order, maintaining that the investigation serves a dual purpose of counterintelligence and criminal investigation. n255 This is directly contrary to the intent of FISA. n256 FISA should be amended to exclude from any criminal trial evidence obtained from a FISA surveillance after there was probable cause to believe that a crime was being committed. This will require the FBI to obtain a Title III order at the appropriate time, making the wiretap subject to the higher standards applicable to Title III intercepts.

-----Footnotes-----

n253. See Foreign Intelligence Surveillance Act: Hearings before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary, 98th Cong., at 27-35 (1983) (testimony of Mark H. Lynch, American Civil Liberties Union).

n254. See McGee & Duffy, *supra* note 78, at 13.

n255. *Id.*

n256. S. Rep. No. 95-604 (1978).

-----End Footnotes-----

IX. International Issues

The Internet is a global medium. One of its great strengths is the ease with which it spans the globe: information flows as effortlessly from New York to Nairobi as from one building to another in Washington, D.C. Moreover, a communication from New York to Nairobi might travel through the United Kingdom

and five other countries one day, but through France and five different countries the next. In this global context, it has been said, the U.S. Bill of Rights is a local ordinance, meaning that the U.S. constitutional guarantees (and the procedures of the U.S. wiretap laws) offer no privacy protection against foreign government interception of the communications of U.S. citizens that cross national borders.

As U.S. law enforcement agencies become more active abroad, and as they engage in more joint operations with foreign police organizations, the line blurs between intelligence agencies and law enforcement agencies. Greater attention will have to be paid to the rules governing electronic surveillance abroad. For both the Internet and traditional telephony, new rules need to be developed to govern U.S. surveillance abroad and the increasing extent of joint international operations, which currently take place in a legal no-man's-land. It has been held that the U.S. wiretap statutes have no extraterritorial application. n257 Congress should address this gap by extending the court order requirements of Title III and FISA to interceptions of communications by the U.S. government abroad for use in U.S. criminal cases.

-----Footnotes-----

n257. See United States v. Barona, 56 F.3d 1087 (9th Cir. 1995); United States v. Peterson, 812 F.2d 486, 492 (9th Cir. 1987).

-----End Footnotes-----

[*117]

U.S. government agencies, particularly the FBI, have been promoting the adoption of CALEA-type standards on an international scale. In 1994, the "Barrett Commission" in Australia, crediting the FBI's leadership, supported the development of "international user requirements" as the most effective means of "international cooperation to ensure that law enforcement's needs are taken into account in the development of new technology." n258 In 1995, the Council of the European Union adopted a set of interception requirements for telecommunications systems, similar to the requirements developed by the FBI, and urged member states to implement the requirements with respect to systems and service providers in their own countries. n259 Efforts were also undertaken to urge other countries to adopt the requirements. In 1997, the Telecommunications Standardization Sector of the International Telecommunication Union, upon a motion by Australia, adopted a resolution directing all its standards groups to consider the EU surveillance requirements in their standards development. n260

-----Footnotes-----

n258. P.J. Barrett, Review of the Long Term Cost Effectiveness of Telecommunications Interception (Mar. 1994).

n259. Council of European Union Resolution of 17 January 1995 on the Lawful Interception of Telecommunications, (96/C329/01).

n260. ITU, Document C97/58-E (May 9, 1997).

-----End Footnotes-----

If the U.S. government is promoting surveillance standards for systems abroad, it should be U.S. policy to also promote world-wide adoption of privacy protections at least as strong as those in the United States.

U.S. government has been less successful in promoting international adoption of key recovery for encryption. Despite the Administration's best efforts, international bodies have not endorsed key escrow solutions. n261 The OECD Cryptography Policy Guidelines specifically do not endorse key escrow; rather, they cautiously propose that "national cryptography policies may allow lawful access to plaintext or cryptographic keys" n262 (emphasis added).

-Footnotes-

n261. John Markoff, U.S. Fails to Win Global Accord on Police Internet Eavesdropping, N.Y. Times, Mar. 27, 1997, at D1. See Jennifer L. Schenker, EU Is Expected to Reject U.S. Proposal for Monitoring Internet Communications, Wall St. J., Oct. 8, 1997, at B9.

n262. Organization for Economic Cooperation and Development, Recommendation of the Council Concerning Guidelines for Cryptography Policy (Mar. 27, 1997).

-End Footnotes-

Nonetheless, as market-driven key escrow arrangements emerge, Fourth and Fifth Amendment concerns about what standards will govern access to keys take on international implications, because governments will be seeking access to keys escrowed outside their territory. If commercial key escrow systems achieve acceptance in the United States, foreign governments are likely to seek access to escrowed keys and decryption assistance, raising the question of standards to be applied when a foreign government seeks cooperation of U.S. authorities. To regulate any assistance provided to foreign governments seeking access to escrowed keys or decryption assistance in the United States, and to prevent the disclosure of decryption keys or decryption assistance to foreign governments that do not respect privacy and other human rights or provide due process, Congress should adopt statutory rules that include strict court order standards. The rules for a foreign request should have to satisfy three basic criteria: 1) the foreign government should comply with the treaty and other standards normally governing the provision of U.S. legal assistance to that government; 2) the foreign request should have to meet a standard at least as high as U.S. law enforcement agencies; and 3) standards should be in place that prohibit the disclosure of keys or decryption assistance for political offenses or other activity that would be protected under the U.S. First Amendment, or to foreign governments that do not adhere to minimum standards of due process and privacy protection.

X. Conclusion

Communications privacy is a bedrock constitutional principle, and electronic communications must be protected through strong privacy legislation implementing the Fourth Amendment's requirements. For the past quarter century, the law of this nation regarding electronic surveillance has sought to balance the interests of privacy and law enforcement. The uses of new technologies, however, are always outpacing the law, often in ways that threaten privacy, and also in ways that limit law enforcement's effectiveness. Other changes in technology offer the possibility of enhancing privacy. Still other changes increase

surveillance capabilities. Consequently, Congress has been required periodically to examine the legal framework for protecting privacy while ensuring that law enforcement has the necessary and appropriate capabilities. It did so in 1968 when it responded to widespread eavesdropping by prohibiting wiretapping without a [*119] order. n263 It did so in 1986 with the adoption of ECPA, which extended the protections and authorities of Title III to e-mail and cellular telephone communications. n264 It did so again in 1994 when it responded to law enforcement concerns about the impact of new technologies by enacting CALEA, which required telecommunications carriers to ensure that their systems could accommodate government surveillance. I have argued here that it must do so again, to protect privacy.

-----Footnotes-----

n263. Omnibus Crime Control and Safe Streets Act of 1968, tit. III, Pub. L. No. 90-351, 82 Stat. 212 (codified at 18 U.S.C. 2510 et. seq.).

n264. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in sections of 18 U.S.C. 2510-21, 2701-10, 3121-26).

-----End Footnotes-----

As exemplified by the Internet, the digital communications technologies are flexible, decentralized, networked, open and interactive. They merge voice, data, and images. They eliminate distinctions between what is kept in the home and what is stored with third parties. They generate large quantities of easily captured transactional data, combine wireless and wireline systems seamlessly, and place choices and control in the hands of users. Their economics are characterized by competition and innovation. They are global in reach. The explosion in the amount of information transmitted and stored electronically and the emergence of a form of online existence for both businesses and individuals have produced a qualitative change in the nature of communications and, accordingly, in the amount and nature of the information that is exposed to intrusion, interception and misuse. A re-examination of the wiretap laws must take into account these defining features of the digital revolution.

With a review should also consider the overall balance between the technical and legal capabilities of government and the technical and legal status of privacy protections. Piecemeal amendments to the surveillance laws in response only to government concerns will inappropriately upset the balance. Any amendments to the wiretap laws must be narrowly crafted to ensure that they do not erode privacy protections, and must be balanced by other, privacy-enhancing amendments. New technologies enhance the ability of law enforcement to intercept and analyze communications and track individuals. Many of these enhancements are coming about without government intervention, as the unintended consequences of market-driven changes in technology. Existing law allows law enforcement to take advantage of these developments. As technology enhances surveillance capabilities, [*120] the legal standards for government use of these new technologies must be increased to adequately protect privacy. I have recommended here a number of amendments that respond to technological changes to protect against abuse without curtailing legitimate law enforcement access.

Government efforts to control the development of technology to preserve its communications surveillance capability must be carefully circumscribed. Merely as a practical matter, the rapid and decentralized changes occurring in

technology are likely to outstrip government efforts at control. The most notable case in point is encryption: there seems to be no way to limit the spread of virtually unbreakable encryption. Changes in technology since 1994 when Congress adopted the CALEA legislation pose equally difficult problems, while also creating opportunities for enhancing privacy. Congress and the FCC should restrain FBI efforts to use this legislation to obtain surveillance capacities that go beyond the status quo.

The legislature must continually strive to develop rules that keep pace with technological developments. The process never reaches a point of final repose, but there are clear steps that should be taken now to reestablish the balance between privacy and government surveillance powers.

LORD, JOHN J. DUNHAM, RONALD W. GRAY, JOHN MENEGUZZO, LISA J. MENEGUZZO, VINCE LEE, CYNTHIA DUBEY, ANTHONY CONSOLINI, VIVIAN SAMBUCCO, SCOTT BULEY, BEVERLY POLVINO, CARL FITZGIBBONS, DALE TATEM, GAETANO MARINO, TERRY L. GROEPER, JOSEPH ALBUQUERQUE, JULIE S. ALBUQUERQUE, JOSEPH LONGO, ROBERT QUICK, JOHN CLEARY, JAMES BRADLEY, TERRY L. GROEPER, JOE E. GORMAN, PAUL TORBICKI, PATRICIA J. HUNDT, WILLIAM GILDERSLEEVE, JANE E. WALTON, DON DYBVICK, PETER M. O'BRIEN, HOWARD J. OSTERHOUT, DAVID COLEMAN, KYLE A. TABER, RAYMOND E. KING, RODNEY CLEMENT, MICHAEL L. BOCHICCHIO, DAVID CAREY, GERARD CHARTIER, THEODORE DEROUIN, WILLIAM DWYER, HARRY MOTTRAM, RICHARD D. NICHOLSON, ORMONDE OSBORNE, ROBERT L. OUSTERHOUDT, JOHN RAGAZZI, ORLANDO RAMIREZ, PATRICK T. GRAHAM, JOE LAPUT, THOMAS SHIA, KENNETH STARTZ, ROBERT ANGER, THOMAS NICOLETTI, R.W. KRYSIAK, DAVID O'KEEFE, CHARLES REVOIR, SERGE SAMAL, ROBERT ROSS, THOMAS PIETRINI, MICHAEL COPE, RICHARD D. NICHOLSON, LARRY AHEARN, DAVID BARGER, MICHAEL BOLTON, DAVID DEVITO, JOSEPH DAVID DYNDERSKI, LEE M. ELLIOTT, JULIO FERNANDEZ, JR., RICHARD B. FORD, RICHARD W. GARDNER, KENNETH GOUGH, MICHAEL GRAHAM, CHARLES E. GUNN, R.W. KRYSIAK, JOSEPH LAPUT, MARTIN LANE, WILLIAM ROBERT MACINTOSH, WILLIAM MACLEAN, MALCOLM R. MAJOR, HENRY MAYNARD, WILLIAM MCCASLAND, CARMELO OTERO, CHARLES OUELLETTE, KEVIN A. RODINO, STEVE SALVATORE, WILLIAM SOUKUP, PETER STRNISTE, MARTINIQUE ZHIGAILO, ALEXANDER JONES, DWIGHT CARLSON, ERWIN MCKINNEY, DAVID HUTCHINSON, TERRENCE DUNN, DAVID WADDELL, FREDERICK DOWNS, EUGENE TERRY, JAMES ROGERS, SANDRA BROWN, JOHN HILL, DONALD F. LOPRESTO, RAYMOND W. SHOVE, III, GEORGE M. LAWRENCE, KENNETH WILSON, ANGELO F. TOSI, MARIO A. GAROFALO, WILLIAM J. BARBOUR, DONALD BARRY, ROBERT BIRGE, PETER L. CONSIDINE, ENRICO G. SOLIANI, HOWARD SMITH, PETER R. TERENCE, III, KEVIN MCCARTHY, BARRIE TOOTHILL and ARTHUR VON HOLTZ, Intervenor-Plaintiffs-Appellees, v. LESTER J. FORST, JOHN A. MULLIGAN, JOHN JACEWICZ, MICHAEL STERGIO, WARREN T. SEELEY, RAOUL OULLETTE, FREDERICK DIGGLE, THOMAS ELLIOTT, WILLIAM SMITH, EDWARD DAILEY, PETER PLANTE, ROBERT OFFEN, ROBERT O'SHAUGHNESSY, CHARLES LEVY, JAMES HILTZ, TIMOTHY BARRY, RICHARD LEVINE, RUBIN BRADFORD, JAMES REILLY, STATE OF CONNECTICUT, JOSEPH FAUGHNAN, WALTER SCHOLTZ, JOHN F. WATSON, GEORGE MOORE, DONALD PAIGE, JOHN BARDELLI, ROBERT BESSECHER, WILFRED BLANCHETTE, HENRY BOURGEOIS, VINCENT BRENNAN, MANFRED BRIDEAU, RICHARD BROZEK, JOHN BURKE, JOHN E. BRYMER, SHAUN BYRNE, JOHN CAPUTO, DOMINIC CONSOLE, RICHARD COVELLO, FRANK D'AMICO, JAMES DARBY, RICHARD DAY, JOHN DEWEY, JOHN FOLEY, CHRISTOPHER GARRITY, ERROL GOFFE, PAUL GUILLOT, BRUCE HAINES, PATRICK HEDGE, DORRIS HUGHES, ROBERT HULL, GEORGE HUSTON, PAUL JASKOLKA, ANTHONY KALKUS, PETER J. KENNEDY, THOMAS KENNEY, CORNELIUS KERWIN, WILLIAM KIRKBY, KENNETH KIRSCHNER, JOHN LEONARD, JOHN LEONE, DONALD LONG, PAUL L. MALLON, DOUGLAS MANAHAN, RICHARD MAYNARD, JOHN MCGOLDRICK, JAMES McGRATH, LAWRENCE MERRILL, RONALD MIKULKA, JAMES MOONEY, BERNARD MORAN, ROGER MORGAN, CHARLES A. MORRISON, JR., RAYMOND MORSE, JOHN MUCHERINO, LIEUTENANT MYERS, DONALD NURSE, SCOTT O'MARA, DAVID PAIGE, JOSEPH PALOMBIZIO, JOSEPH PERRY, JOHN REARICK, TROOPER REED, JAMES RICE, RICHARD RIZZUTI, FRANK ROBINSON, JOHN ROFSKY, JAMES ROGERS, ROBERT ROOT, ROYAL SCHIFFER, JAMES SHAY, JAMES SMITH, CHARLES SUPSINSKAS, WILLIAM SYDENHAM, JOHN TAYLOR, MATTHEW TYSKA, RAYMOND WATROUS and ROBERT WELCH, Defendants-Appellants.

Docket No. 95-7614

UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

88 F.3d 111; 1996 U.S. App. LEXIS 15951

December 21, 1995, Argued

July 3, 1996, Decided

PRIOR HISTORY: [**1] Appeal by defendants from an order of the United States District Court for the District of Connecticut, T.F. Gilroy Daly, Judge, denying motion for summary judgment based on qualified immunity from claims relating to State Police practice of tape-recording telephone calls to, from, and within state police barracks. See 888 F. Supp. 1235 (1995). Motion by plaintiffs to dismiss

for lack of appellate jurisdiction.

DISPOSITION: Motion granted; appeal dismissed for lack of jurisdiction.

CORE TERMS: recording, conversation, telephone, summary judgment, recorded, listening, qualified immunity, tape, listened, barracks, arrestee, qualified-immunity, immunity, beep, confidential conversations, tone, warning, labels, incoming, outgoing, trooper, immediately appealable, interception, unrecorded, wire, automatically, state law, attorney-client, confidential, intercepted

COUNSEL: AARON S. BAYER, Deputy Attorney General, Hartford, Connecticut (Richard Blumenthal, Attorney General of Connecticut, Henri Alexandre, Carolyn K. Querijero, Jane R. Rosenberg, Assistant Attorneys General, Hartford, Connecticut, John W. Sitarz, Cooney, Scully & Dowling, Hartford, Connecticut, on the brief), for Defendants-Appellants.

CHRISTOPHER D. BERNARD, Bridgeport, Connecticut (Koskoff, Koskoff & Bieder, Bridgeport, Connecticut, Garrett M. Moore, Judith A. Mauzaka, Moore & O'Brien, Cheshire, Connecticut, on the brief), for Plaintiffs-Appellees and Intervenors-Plaintiffs-Appellees.

JUDGES: Before: KEARSE, MAHONEY, and PARKER, Circuit Judges.

OPINIONBY: KEARSE

OPINION:

[*114] KEARSE, Circuit Judge:

Defendants Lester [*2] J. Forst and other present and former officials of the Connecticut State Police ("State Police") appeal from so much of an order of the United States District Court for the District of Connecticut, T.F. Gilroy Daly, Judge, as denied their motion for summary judgment dismissing claims brought principally under 42 U.S.C. § 1983 (1994) and Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520 (1994) ("Title III"), alleging that between 1978 and 1989 the State Police intercepted, recorded, disclosed, and used, without knowledge or consent of the participants, all telephone calls made to, from, and within State Police barracks, in [*115] violation of, inter alia, Title III and the Fourth, Fifth, Sixth, and Fourteenth Amendments to the United States Constitution. The defendant officials sought summary judgment principally on the ground that they were entitled to qualified immunity. The district court denied that part of their motion on the ground that the rights of individual plaintiffs under the above laws were clearly established and that there are genuine issues to be tried as to pertinent factual issues, including (a) whether plaintiffs consented [*3] to the recording, and (b) whether and to what extent the State Police listened to any given recorded conversation. On appeal, defendants contend that they are entitled to qualified immunity principally because at the pertinent times it was not clearly established that tape-recording telephone calls, without ever listening to them, violated Title III or the federal Constitution or state law. Plaintiffs have moved to dismiss the appeal for lack of appellate jurisdiction. For the reasons below, we agree with plaintiffs that because the district court denied summary judgment on the ground that there existed questions of fact to be tried with respect to the qualified-immunity defense, the denial was not an immediately appealable order, and we therefore dismiss the appeal for lack of jurisdiction.

I. BACKGROUND

This class action, a consolidation of several lawsuits, began in November 1989 after the public learned that for more than a decade the State Police had engaged in a practice of automatically recording telephone calls made on lines in each of its barracks. The plaintiff class, as certified by the district court, comprises all persons who participated in telephone calls to, from, [*4] or within State Police facilities between January 1, 1978, and November 9, 1989, whose calls were intercepted, recorded, and/or used by defendants in violation of law. The court also certified a plaintiff subclass of current and former State Police employees, other than those named as

defendants, who participated in such calls.

The background of the litigation is set forth in detail in the district court's published opinion, see 888 F. Supp. 1235 (1995), and will be summarized here only to the extent pertinent to this appeal. Many of the facts are not in dispute.

A. The State Police Policy and Practice of Recording Calls

The State Police is divided into three districts, each comprising four troops; each troop occupied its own barracks. In or before mid-1978, the State Police installed tape recorders on telephone lines in all 12 barracks plus its Headquarters Message Center. As explained by defendants, the tapes of the recordings "could be referred to in the ordinary course of police business and in furtherance of official police duties" in order to "investigate complaints made by the public against State Police personnel, e.g., internal affairs investigations"; or to **[**5]** "permit dispatchers to replay a communication when the message was not clear, e.g., to hear the street number"; or to "be used in major criminal investigations, e.g., to establish the time a complaint was received and when follow-up responses were made"; or to permit "a quality control check by the inspections unit to determine if the dispatchers and troopers were handling calls properly." (Defendants' Statement of Undisputed Facts P 6.)

The machines installed by the State Police recorded incoming and outgoing calls indiscriminately. Although a 1978 State Police manual on wiretapping stated that a "call between a lawyer and a client presently the subject of criminal charges can under no circumstances be monitored," Office of the Chief State's Attorney Special Investigations Division Manual on **Wire Tapping** (1978) ("**1978 Wire Tapping Manual**"), when persons were arrested or detained and wished to call their attorneys, they were directed to a barracks telephone on which all conversations were routinely recorded. Nor did the State Police make any effort not to record incoming calls from attorneys to their clients.

It was known by the State Police when these recording systems **[**6]** were installed, and at all subsequent times, that they recorded both incoming and outgoing calls; that they recorded specific telephone lines (onto which calls from all telephone **[*116]** handsets were routed automatically) rather than specific telephone handsets; and that there existed no unrecorded lines dedicated for use by detainees, arrestees or suspects.

888 F. Supp. at 1244 (emphases added).

Though the recorders used in the early years of the pertinent period used "beep tones" to alert call participants that their conversations were being recorded, "by 1986 . . . some recorded lines did not have beep tones." Id. at 1243. Although defendants asserted that the public was also on notice as to the recording practice because of statements in local area telephone books that calls to police, fire, and other emergency facilities could be recorded, the district court noted that this alert did not mention calls made from, rather than to, such facilities.

In 1983, the Connecticut Supreme Court decided State v. Ferrell, 191 Conn. 37, 463 A.2d 573 (1983) ("Ferrell"), which involved a murder conviction based, in part, on statements made by the defendant during one of two **[**7]** telephone conversations with his attorneys. Ferrell's incriminating statements were recounted at trial by State Police troopers who had heard his side of the conversation because the telephone they allowed him to use was in the barracks report room. Though the tape recordings of Ferrell's conversations were not admitted into evidence, a state trooper testified, apparently in an effort to show that when Ferrell spoke to his attorneys he had no reasonable expectation of privacy, that the calls were recorded and that there were periodic beeps to warn participants of the recording. The tapes were reviewed by the Connecticut Supreme Court, which found that in fact the recording of the defendant's call to his first attorney did not register a beep tone, and that the recording of an incoming call from his second attorney contained only "muted warning beeps." Id. at 39 n.2, 463 A.2d at 575 n.2. The court stated that although Ferrell's

statements were not obtained by police interrogation or by "coercive measures appearing on the record," id. at 42, 463 A.2d at 576. Ferrell clearly had indicated his intention not to give the police a statement, and the interception of his statements [**8] to his attorney resulted in the very sort of self-incrimination that Miranda warnings are meant to guard against. The court ruled that the admission of the statements violated Ferrell's due process and Miranda rights. It stated that when access to an attorney is provided, "privacy must be ensured." Id. at 44, 463 A.2d at 578.

In the wake of Ferrell, defendant Ronald Mikulka, the State Police telecommunications chief, sent defendant Donald Nurse, head of the central district, a memorandum reflecting media comment on the Ferrell decision and suggesting that arrestees could be provided with an unrecorded line for calls to their attorneys:

The attached article in the HTFD Courant (8/10/83) indicates that Police are obliged to provide a private telephone for accuseds to consult with their attorney. We should have a clear policy on this situation. If necessary we will arrange for the proper phone equipment. There are several options available. The simplest would be to provide a separate phone set with a local line that could be kept in the interrogation room and jacked in when needed.

(Mikulka memorandum dated August 11, 1983.) Notwithstanding this [**9] suggestion,

Mikulka received no response to this memorandum, and he took no further steps to determine whether the State Police were recording attorney-client telephone calls. Indeed, at no time prior to November 1989 did the State Police enunciate a formal policy to assure an arrestee was provided access to an unrecorded telephone line.

888 F. Supp. at 1245.

In 1984, State Police Commissioner Forst requested an opinion from the Connecticut Attorney General with respect to the legality of intercepting wire or oral communications in a hostage or terrorist situation. He received an opinion indicating that no wire interceptions whatever were proper without judicial authorization:

we conclude you may not intercept wire communications even in these circumstances without a warrant.

(Letter from Connecticut Attorney General Joseph I. Lieberman to Commissioner Forst [*117] dated March 24, 1986, at 1 (emphasis added).)

In 1986, defendant John A. Mulligan, Forst's second-in-command, decided that, with the exception of the troop commander's private line and the informant's lines, recordings should still be made of all incoming and outgoing telephone lines. He also [**10] decided that the beep tones should be removed on all recorders and replaced by warning labels. Although such labels were eventually ordered and distributed, plaintiffs contend that in some barracks there was a period during which the beep tones had been eliminated and the labels had not yet been affixed; that in other barracks labels were promptly affixed but were not replaced after they had become worn or had been removed; and that in still others, warning labels were never affixed.

In January 1988, a revised State Police Administration and Operations Manual ("1988 Operations Manual") stated for the first time that recording machines had been installed in all barracks and the Headquarters Communications Section to record all radio and telephone conversations transmitted or received. It did not provide any guidelines covering the use of beep tones, warning labels, or other

notification or consent procedures.

As noted, the tapes created by the State Police system did not distinguish between incoming and outgoing calls. Further, there was no way to determine, without listening to the tape, where a given call began and ended. Thus, when an officer

reviewed tapes for administrative [**11] purposes[, he] generally took tapes from the barracks to a separate location, usually headquarters, and spent a full day reviewing them. . . . All internal investigations or inspections required a trooper to search for a conversation on a particular tape by listening to the entire tape until the specific conversation was identified. If information obtained in a tape recording was relevant to an internal affairs investigation, the tape could be used against the employee in departmental hearings.

888 F. Supp. at 1246 (emphases added).

In 1989, the State Police recording practices came to the public's attention as a result of testimony given by a trooper on cross-examination in a pretrial hearing in *State v. Little*, CR4-156380, MV4-298174 (Nov. 3, 1989). The testimony revealed that after Little's arrest following a traffic accident, he had made four telephone calls from the barracks to which he had been taken, two to family members and two to his attorney. The calls had been recorded without his consent and without notice to him:

No warning labels existed in the barracks or on the telephones themselves, there was no audible beep tone on the line [**12] Little used, and Little was neither advised of the recording nor told that he could have access to an unrecorded line.

888 F. Supp. at 1246-47; see also Deposition of State Police trooper Maryann Daley at 286.

These disclosures caused an uproar in the media, and the Governor called for and received Forst's immediate resignation. The district court noted that

following his resignation Forst stated in an interview that both he and Mulligan were unaware that the recording system was recording all telephone calls, including those between suspects and their attorneys,

888 F. Supp. at 1247 n.12, and that Mulligan similarly stated, "I think every single person of the management staff thought that there were lines available for conversations that were non-recorded," *id.* (quoting newspaper article quoting Mulligan).

B. The Denial of Defendants' Summary Judgment Motion

The plaintiffs in the present action include persons who were arrested by the State Police and made or received telephone calls while being detained at State Police barracks and criminal defense attorneys who made and received calls to and from their clients who were being detained [**13] at State Police barracks. The complaint, as amended through May 1991, alleged that defendants had engaged [**118] in a widespread and secret program to intercept, record, disclose, or use wire and oral communications, in violation of numerous federal and state statutory and constitutional provisions. It demanded, *inter alia*, compensatory and punitive damages from the individual defendants in their individual capacities, an injunction prohibiting the defendant officials and the State of Connecticut from continuing to conduct unauthorized recording, and an injunction

prohibiting disclosure of any recording without a court order.

After extensive discovery, the individual defendants moved for summary judgment on the principal grounds (1) that plaintiffs could not sustain their burden of establishing that the defendants violated any of their federal or state rights, and (2) that defendants were entitled to qualified immunity. With respect to the claims that are pertinent to this appeal, to wit, plaintiffs' claims under Title III, the Fourth, Fifth, Sixth, and Fourteenth Amendments to the United States Constitution, and various provisions of state law, defendants asserted that they had not [**14] violated any clearly established rights of the plaintiffs of which a reasonable person would have known and that it was objectively reasonable for defendants to believe that their actions did not violate any clearly established rights. Defendants acknowledged that the goal of the State Police had been to record all conversations on barracks telephone lines available to the public and that taped telephone lines were used for both incoming and outgoing calls. In support of their motion, however, defendants stated, inter alia, that the purposes of the recording were to permit review of emergency calls when the message was not clear, to facilitate investigation of civilian complaints against State Police personnel, to establish the timing of complaints and official responses in major criminal investigations, and to determine whether dispatchers and troopers were handling calls properly. (Defendants' Statement of Undisputed Facts P 6.) Defendants stated that

only a relatively few recordings of conversations were ever listened to at all, and those few were listened to only by authorized police personnel for the legitimate police purposes described in paragraph 6, above. All others [**15] were routinely erased and taped over without ever being heard. . . .45. There was no intent on the part of the Connecticut State Police or individual officers specifically to record any attorney/client telephone conversations, and to the extent that such conversations may have been recorded it was a by-product of the overall system which automatically recorded all calls, and the calls were never designated to be replayed or listened to. . . .48. The State Police did not listen to or replay any attorney/client call which may have been automatically recorded.

(Defendants' Statement of Undisputed Facts PP 44, 45, 48.)

Plaintiffs, opposing summary judgment, disputed defendants' contentions that the State Police did not intend to capture attorney-client conversations and that troopers neither listened to nor replayed such conversations, pointing to the recording and/or use of attorney-client conversations in the Ferrell and Little cases. Plaintiffs also pointed out that

defendants had a policy to permit arrestees and detainees to use State Police telephones to contact their attorneys as well as a policy to record all telephone [**16] calls on State Police lines. This is inconsistent with defendants' statement that they did not intend to record attorney/client conversations.

(Plaintiffs['] and Intervening Plaintiffs' Response to Defendants' Statement of Undisputed Facts P 17.)

In a comprehensive opinion, the district court denied defendants' motion for summary judgment dismissing the Title III, Fourth, Fifth, Sixth, and Fourteenth Amendment, and state law claims, finding principally that there were material questions of fact to be tried as to each claim. With respect to the Fourth Amendment claims, the court noted that the two core questions are whether plaintiffs exhibited a subjective expectation of privacy, and if so, whether that expectation was one that society is prepared to recognize as reasonable. The court indicated [*119] that the first question should likely be answered adversely to defendants and that the second was not answerable as a matter of law:

Defendants first contest that plaintiffs subjectively expected their telephone calls to be private, given that plaintiffs made their calls from a barracks of the State Police. This argument is belied, however, by the fact that both Commissioner Forst [**17] and Colonel Mulligan disavowed any knowledge of the extent of the recording practices of the State Police. If those in charge of the State Police can claim no subjective knowledge of the recording of outgoing calls, it must be expected that plaintiffs do likewise. Defendants also argue that plaintiffs' expectation of privacy was unreasonable. . . . Where no consent exists, and where conversations consist of privileged communications between clients and their attorneys, an expectation of privacy is reasonable. . . . The surreptitious recording of unprivileged but private calls, if proven, involves an invasion of privacy that far outweighs defendants' proffered justifications. . . . Ultimately, therefore, the determination of whether the plaintiffs' expectations of privacy were reasonable depends on proof of the absence of notice, a question of fact precluding summary judgment on plaintiffs' Fourth Amendment claims.

888 F. Supp. at 1255-56 (emphasis added).

With respect to the Fifth Amendment claims, the court noted that offering an arrestee a telephone while knowing that the call would be secretly recorded could be viewed as the functional equivalent of an interrogation [**18] because it would be known to be "reasonably likely to elicit an incriminating response." Id. at 1257 (quoting Pennsylvania v. Muniz, 496 U.S. 582, 601, 110 L. Ed. 2d 528, 110 S. Ct. 2638 (1990)). The court further noted that the privilege against self-incrimination "applies not only to evidence which would support a conviction, but to 'information which would furnish a link in the chain of evidence that could lead to prosecution, as well as evidence which an individual reasonably believes could be used against him in a criminal prosecution.'" 888 F. Supp. at 1257 (quoting Maness v. Meyers, 419 U.S. 449, 461, 42 L. Ed. 2d 574, 95 S. Ct. 584 (1975)). The court concluded that

whether such evidence was ever induced through the recording of private calls, or was ever used derivatively in any criminal proceeding, are matters to be established at trial.

888 F. Supp. at 1257.

With respect to the arrestee-plaintiffs' Sixth Amendment claims, the court stated as follows:

Defendants argue that [the arrestee or detainee] plaintiffs cannot claim the subject matter of their calls was meant to remain confidential, and that in any case any police intrusion caused by the recording was unintentional. As discussed above, however, [**19] a reasonable expectation of privacy might have existed. Moreover, defendants admit to taping all calls, to having no unrecorded lines available, and to directing arrestees to use recorded lines. Any resulting recording cannot be said to be inadvertent, and implicates the Sixth Amendment. . . . As to arrested plaintiffs, therefore, two significant issues remain for trial: whether the communications between arrestees and their attorneys were intended to remain confidential, and whether it was reasonable for these plaintiffs to expect such communications to be confidential. The question of whether any notification mechanisms (beep tones and warning labels) existed will be central to these inquiries.

888 F. Supp. at 1258 (emphasis added).

With respect to the rights of all plaintiffs to privacy, as protected by the Fourteenth Amendment, the

court stated that "the right to privacy is not violated unless an individual's interest in maintaining confidentiality outweighs the government's interest in disclosure," 888 F. Supp. at 1258-59 (citing Nixon v. Administrator of General Services, 433 U.S. 425, 458, 53 L. Ed. 2d 867, 97 S. Ct. 2777 (1977)), but it concluded that none of the governmental interests [**20] described by defendants was sufficient to justify the recording of confidential conversations. The [**120] court noted that plaintiffs nonetheless could not prevail on these claims if they had consented to the interception, and it concluded that the matter of whether or not there was notice sufficient to impute consent was a fact remaining for trial.

With respect to the claims under Title III, defendants argued that the State Police recording system was exempt because the tapes were listened to only to the extent necessary to meet emergency and administrative needs, i.e., uses within the Act's exception for legitimate law enforcement activities, see 18 U.S.C. § 2510(5)(a)(ii). The court noted that plaintiffs contended, inter alia, that the statute was violated by a recorded interception even if defendants did not listen to the conversation, but the court concluded that it need not decide that question because defendants indisputably had listened to some conversations, and whether they had confined that listening to the emergency and administrative matters, as defendants claimed, could not be determined as a matter of law:

The second element of a section 2520 violation is [**21] that a wire, oral, or electronic communication must be intercepted. The statute defines "intercept" to mean "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." 18 U.S.C. § 2510(4). . . . As an initial matter it appears obvious that the defendants' actions often resulted in "interceptions" under any definition of that term. To determine whether the recording of a particular call was needed for emergency or administrative reasons, and hence whether it was an exempt recording under the law enforcement exception, the State Police would delegate a trooper to listen to all calls in a given time period. It is undisputed that the State Police's recorders did not possess the capability to locate a particular call automatically. Even under the defendants' proposed interpretation of "interception," therefore, defendants "aurally acquired" plaintiffs' conversations whenever they listened through tapes searching for particular calls. What specific tapes were listened to, and which conversations were therefore "intercepted," as defendants interpret that term, thus would appear [**22] to be issues of material fact precluding summary judgment in defendants' favor.

888 F. Supp. at 1263-64 (emphases added). Further noting that Title III excepts conversations intercepted with the consent of one of the parties, the court reiterated its rejection of defendants' contention that all users of State Police telephones received adequate notice of the recording system, and it observed that "a genuine issue of material fact exists as to whether plaintiffs' consent to the recording can be implied." 888 F. Supp. at 1265; see also id. at 1266; ("what none of the parties in this case has established, is whether each caller who made a private or privileged telephone call received notice that the conversation was recorded"); id. at 1267 ("it remains a question of fact whether defendants listened to protected conversations while reviewing tapes for other purposes").

The district court concluded that the factual issues precluded summary judgment for defendants on their qualified-immunity defense with respect to any of these claims. The court found that the essential contours of the Fifth and Sixth Amendment rights were sufficiently clear in light of earlier decisions [**23] of the United States Supreme Court and the Second Circuit, and in light of the Connecticut Supreme Court's opinion in *Ferrell*. While noting that in some instances it was not clear that plaintiffs' rights were violated under defendants' view of the facts, the court found that with respect to each of plaintiffs' claims there were fact questions to be determined as to which side's view of the facts was correct. Thus, while defendants contended that it was not clearly established at the pertinent times that the constitutional provisions or Title III made it unlawful to record a telephone conversation if the conversation was never listened to, the court concluded that the matter of whether a given conversation was ever listened to was a question of fact for trial. In addition, the court stated that

the second element of the qualified immunity defense as to the rights of these [*121] plaintiffs rests on disputed issues of fact, precluding summary judgment. Defendants argue, in particular, that notification mechanisms were in place throughout the class period. If such mechanisms were actually implemented and maintained, it would be objectively reasonable for a police officer in defendants' [**24] position to believe that the recording of plaintiffs' private conversations occurred with their consent, and thus no Fourth or Fourteenth Amendment violation occurred. Since the facts relating to notification and plaintiffs' expectations of privacy remain at issue, however, summary judgment on those claims is inappropriate.

888 F. Supp. at 1261 (emphasis added). With respect to privileged or private telephone conversations, the court found it clear that the law-enforcement exception to Title III did not exempt defendants' conduct from the prohibitions of that statute:

Defendants cannot plausibly argue that Congress intended the recording of privileged or private conversations in violation of the Constitution, as alleged in this case, to fall under Title III's definition of "law enforcement duties." In sum, plaintiffs' rights under Title III were defined adequately by court decisions and the Act itself during the period in question, and a reasonable official in defendants' position would have understood that the acts alleged by plaintiffs were unlawful under Title III.

888 F. Supp. at 1267 (footnote omitted).

With respect to defendants' awareness of the [**25] law, the court found it significant that defendants had made some efforts to warn telephone users of recording:

Defendants admit that they attempted to place beep tones on recorded lines when they first initiated recording, thereby acknowledging a duty not to record conversations without notification. This acknowledgement is sufficient to raise the question whether it was objectively reasonable for defendants to believe, throughout the class period, that their recording practices did not violate plaintiffs' Title III rights, given the factual issue whether working beep tones existed on all recorded lines. Defendants therefore fail to establish their qualified immunity defense at this time.

888 F. Supp. at 1268 (emphasis added). As to both constitutional and statutory rights, the court found that in light of the 1986 Attorney General's letter and the 1978 **Wire Tapping** Manual's admonition that under no circumstances could an attorney-client conversation properly be monitored, "no objectively reasonable police officer, so informed, would believe that the recording of conversations between arrestees and their attorneys was lawful" Id. at 1260; see also [**26] id. at 1267-68.

The district court similarly ruled that defendants had not shown entitlement to qualified immunity against the state-law claims, in part because in order to establish that defense, defendants would be required to show that their acts did not "involve malice, wantonness or intent to injure," and that they had no knowledge of the specific harm or injury alleged. Evon v. Andrews, 211 Conn. 501, 505, 559 A.2d 1131, 1134 (1989). The district court stated:

Defendants fail to demonstrate their defense of qualified immunity under state law for the reasons stated in the Court's discussion of federal qualified immunity. While it is true, as defendants note, that the Connecticut Supreme Court has never explicitly assessed the practices alleged here, the Ferrell decision and the Attorney General's 198[6] opinion

letter, in particular, informed defendants that the recording of private or privileged telephone conversations would violate the federal and State constitutions and the State Wiretap Act. Whether defendants' actions also involved "malice, wantonness, or intent to injure," given defendants' decision to remove the beep tones from recorded lines, remains [**27] a question of fact for trial.

888 F. Supp. at 1270 (emphasis added). The court also found summary judgment inappropriate on the state-law claims because "there exists a genuine issue whether, and to what extent, employees of the State Police reviewed and listened to tapes of private conversations." Id. at 1271.

[*122] This appeal followed, challenging so much of the district court's order as denied defendants' motion for summary judgment based on qualified immunity.

II. DISCUSSION

On appeal, the defendant officials argue that they were entitled to summary judgment dismissing the complaint on the ground that reasonable officials could have believed that the State Police taping system was not unlawful because, during the pertinent period, it was not clearly established that Title III or the federal Constitution or state law prohibited the recording of conversations without ever listening to them. Plaintiffs have moved to dismiss the appeal, pointing out that the denial of a summary judgment motion asserting qualified immunity is not immediately appealable unless the denial turned on an issue of law, and that the district court here found numerous genuine issues of material [**28] fact to be tried with respect to the qualified-immunity defense, including the questions of whether and to what extent confidential conversations were listened to and/or used.

As to appealability, defendants contend that the district court's rulings that there are issues of fact to be tried are irrelevant because, defendants say, plaintiffs' claims are based solely on the fact that the calls were recorded, and not on any listening or use. (See, e.g., Defendants' brief on appeal at 32 (referring to recording without any listening as "the claim pursued by these plaintiffs" (emphasis added); *id.* at 34 (stating that "plaintiffs did not even argue . . . that incriminating information was obtained or used through the monitoring of private phone calls").) If defendants were correct in their assertion that plaintiffs claim only that defendants violated their rights by recording conversations, without ever listening to them, the district court's denial of the motion for summary judgment would be immediately appealable, for the issue before us would then turn solely on the purely legal question of whether clearly established law prohibited recording simpliciter. Plaintiffs' [**29] claims are not, however, simply based on defendants' recording without any listening. The complaints alleged that defendants violated plaintiffs' rights by intercepting, recording, disclosing, and using their confidential telephone conversations. And plaintiffs' brief on appeal states that "their allegations are not and have never been limited to a violation based solely on recording" (Plaintiffs' brief on appeal at 16.) Accordingly, defendants' narrow characterization of plaintiffs' claims is a mischaracterization.

As to the merits of their appeal, defendants contend that they are entitled to qualified immunity on the ground that there was no listening by State Police to confidential telephone conversations. Thus, they argue that "recordings of any privileged conversations were erased without being listened to, and . . . in any event were never used against the speaker in any judicial proceedings" (Defendants' brief on appeal at 34); that "plaintiffs did not . . . offer evidence[] that incriminating information was obtained or used through the monitoring of private phone calls" (*id.*); and that there was no evidence or claim that any recorded conversation was ever used [**30] even derivatively in any criminal proceeding (*id.* at 34-35 n.23). We conclude that, in light of the interplay among the principles governing qualified immunity, summary judgment, and appealability, discussed below, defendants' arguments are factually and doctrinally flawed because (a) it is undisputed that the State Police did listen to at least some tapes; (b) on a summary judgment motion made by defendants, the evidence must be viewed in the light most favorable to plaintiffs; (c) defendants' argument that plaintiffs have not proven listening to, or use of, the recorded conversations is misplaced on this appeal because qualified immunity is an affirmative defense as to which defendants have the burden

of proof; and (d) defendants' assertion that plaintiffs cannot prove listening or use goes to the merits of plaintiffs' claims, and a denial of summary judgment because of the existence of triable issues of fact with respect to the merits is not immediately appealable.

A. Qualified Immunity, Summary Judgment, and Appealability

The federal doctrine of qualified immunity protects government officials from [*123] suits against them in their individual capacity for money damages [**31] where "their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known." Harlow v. Fitzgerald, 457 U.S. 800, 818, 73 L. Ed. 2d 396, 102 S. Ct. 2727 (1982); see also Anderson v. Creighton, 483 U.S. 635, 640, 97 L. Ed. 2d 523, 107 S. Ct. 3034 (1987). A right whose existence is indicated by prior case law with "reasonable specificity" is "clearly defined" within the meaning of this doctrine. See, e.g., Jermosen v. Smith, 945 F.2d 547, 550 (2d Cir. 1991), cert. denied, 503 U.S. 962, 118 L. Ed. 2d 211, 112 S. Ct. 1565 (1992). Further, though officials are not required "to anticipate subsequent legal developments," Harlow v. Fitzgerald, 457 U.S. at 818, a right may have been clearly defined even if the defendants' specific action had not previously been held unlawful if, "in the light of pre-existing law, the unlawfulness [of the action was] . . . apparent," Ayeni v. Mottola, 35 F.3d 680, 686 (2d Cir. 1994) (quoting Anderson v. Creighton, 483 U.S. at 640), cert. denied, 131 L. Ed. 2d 554, 115 S. Ct. 1689 (1995). Even if the right in question was clearly established at the time of the alleged violation, however, the defendants may nonetheless establish immunity by showing that reasonable persons in their [**32] position would not have understood that their conduct was within the scope of the established prohibition. See, e.g., Harlow v. Fitzgerald, 457 U.S. at 818; Robison v. Via, 821 F.2d 913, 921 (2d Cir. 1987).

Qualified immunity is an affirmative defense that the defendants have the burden of raising in their answer and establishing at trial or on a motion for summary judgment. Gomez v. Toledo, 446 U.S. 635, 640, 64 L. Ed. 2d 572, 100 S. Ct. 1920 (1980); see also Harlow v. Fitzgerald, 457 U.S. at 815; Oliver Schools, Inc. v. Foley, 930 F.2d 248, 253 (2d Cir. 1991). On a motion for summary judgment, of course, the moving party has the burden of showing that no genuine issue of material fact exists and that the undisputed facts entitle him to judgment as a matter of law, see, e.g., Adickes v. S.H. Kress & Co., 398 U.S. 144, 157, 26 L. Ed. 2d 142, 90 S. Ct. 1598 (1970), and in ruling on such a motion, the district court must draw all factual inferences in favor of, and take all factual assertions in the light most favorable to, the party opposing summary judgment, see, e.g., Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 255, 91 L. Ed. 2d 202, 106 S. Ct. 2505 (1986); Rodriguez v. City of New York, 72 F.3d 1051, 1061 (2d Cir. 1995). Summary [**33] judgment dismissing a claim on the basis of the defendants' qualified-immunity defense may thus be granted if the court finds that the asserted rights were not clearly established, or if the evidence is such that, even when it is viewed in the light most favorable to the plaintiffs and with all permissible inferences drawn in their favor, no rational jury could fail to conclude that it was objectively reasonable for the defendants to believe that they were acting in a fashion that did not violate a clearly established right. See, e.g., Robison v. Via, 821 F.2d at 921; Halperin v. Kissinger, 257 U.S. App. D.C. 35, 807 F.2d 180, 189 (D.C. Cir. 1986) (Scalia, J., sitting by designation).

Because the defense of qualified immunity is designed to relieve government officials of the burdens of litigation as well as of the threat of damages, summary judgment is encouraged as a device for disposing of claims barred by such immunity. See, e.g., Harlow v. Fitzgerald, 457 U.S. at 818; Ying Jing Gan v. City of New York, 996 F.2d 522, 532 (2d Cir. 1993); Cartier v. Lussier, 955 F.2d 841, 844 (2d Cir. 1992); Kaminsky v. Rosenblum, 929 F.2d 922, 925 (2d Cir. 1991); see also Behrens [**34] v. Pelletier, 133 L. Ed. 2d 773, 116 S. Ct. 834, 842 (1996). For much the same reason, although the denial of summary judgment is ordinarily not an appealable "final decision" within the meaning of 28 U.S.C. § 1291 (1994), see, e.g., Johnson v. Jones, 132 L. Ed. 2d 238, 115 S. Ct. 2151, 2156 (1995) (the question of whether the evidence adduced by the plaintiff is sufficient to show a genuine triable issue of material fact on the merits of his claim, for example, is not reviewable by appeal from the order denying summary judgment), a limited exception has been carved out for certain [*124] summary rejections of the qualified-immunity defense.

In Mitchell v. Forsyth, 472 U.S. 511, 86 L. Ed. 2d 411, 105 S. Ct. 2806 (1985) ("Mitchell"), the

Supreme Court ruled that where a summary judgment motion is based on a substantial claim of qualified immunity, the district court's denial of the motion is immediately appealable under the Cohen doctrine (see Cohen v. Beneficial Industrial Loan Corp., 337 U.S. 541, 93 L. Ed. 1528, 69 S. Ct. 1221 (1949)), if the denial turned on an issue of law. See, e.g., Mitchell, 472 U.S. at 530; Magnotti v. Kuntz, 918 F.2d 364, 367 (2d Cir. 1990); see also Johnson v. Jones, 115 S. Ct. at 2156. To be appealable under the [**35] Cohen doctrine,

the order must [1] conclusively determine the disputed question, [2] resolve an important issue completely separate from the merits of the action, and [3] be effectively unreviewable on appeal from a final judgment.

Coopers & Lybrand v. Livesay, 437 U.S. 463, 468, 57 L. Ed. 2d 351, 98 S. Ct. 2454 (1978). Applying Cohen's criteria, the Mitchell Court reasoned that the rejection of a qualified-immunity defense as a matter of law should be immediately appealable because the qualified-immunity doctrine

recognizes an entitlement not to stand trial or face the other burdens of litigation, conditioned on the resolution of the essentially legal question whether the conduct of which the plaintiff complains violated clearly established law. The entitlement is an immunity from suit rather than a mere defense to liability; and like an absolute immunity, it is effectively lost if a case is erroneously permitted to go to trial.

472 U.S. at 526 (emphasis in original). Once the trial is held, it is too late to vindicate that important purpose of qualified immunity, i.e., allowing the official to avoid standing trial, and the denial is, to that extent, "effectively [**36] unreviewable." Id. at 527. Further, to the extent that the denial of summary judgment turns on a legal issue, the qualified-immunity question is sufficiently separate from the merits of the action that the

appellate court reviewing the denial of the defendant's claim of immunity need not consider the correctness of the plaintiff's version of the facts, nor even determine whether the plaintiff's allegations actually state a claim. All it need determine is a question of law: whether the legal norms allegedly violated by the defendant were clearly established at the time of the challenged actions or, in cases where the district court has denied summary judgment for the defendant on the ground that even under the defendant's version of the facts the defendant's conduct violated clearly established law, whether the law clearly proscribed the actions the defendant claims he took.

Id. at 528. The Mitchell Court took pains to make clear that the denial of a claim of qualified immunity may appropriately be appealed immediately only

"to the extent that it turns on an issue of law." . . . It "emphasized . . . that the appealable issue is a purely legal [**37] one: whether the facts alleged . . . support a claim of violation of clearly established law." . . . It distinguished precedent not permitting interlocutory appeals on the ground that "a qualified immunity ruling . . . is . . . a legal issue that can be decided with reference only to undisputed facts and in isolation from the remaining issues of the case." . . . And, it explained its separability holding by saying that "an appellate court reviewing the denial of the defendant's claim of immunity need not consider the correctness of the plaintiff's version of the facts."

Johnson v. Jones, 115 S. Ct. at 2156 (quoting Mitchell, 472 U.S. at 528 n.9, 530 (emphasis in

Johnson)). Thus, where the district court has ruled that adjudication of the immunity defense requires the resolution of genuinely disputed questions of fact, the denial of summary judgment is not immediately appealable. See, e.g., Cook v. Sheldon, 41 F.3d 73, 78-79 (2d Cir. 1994); Kaminsky v. Rosenblum, 929 F.2d at 926-27; Hurlman v. Rice, 927 F.2d 74, 79 (2d Cir. 1991); Langley v. Coughlin, 888 F.2d 252, 254 (2d Cir. 1989); Mahoney v. Hankin, 844 F.2d 64, 68-69 (2d [*125] Cir. [**38] 1988). To be appealable immediately, the qualified-immunity denial must present "a legal issue that can be decided with reference only to undisputed facts and in isolation from the remaining issues of the case." Johnson v. Jones, 115 S. Ct. at 2156 (quoting Mitchell, 472 U.S. at 530 n.10).

In the present case, defendants concede that, to a certain extent, plaintiffs' federal rights were clearly established; but they argue that what was established was a prohibition against listening to confidential conversations, not against recording without any listening, and they assert that in the present case there was no such listening. For example, they term "unsurprising" the district court's "conclusion that the law was clearly established that: (1) arrestees have a right to confidential communication with their attorneys; and (2) individuals with a reasonable expectation of privacy have a right to keep their telephone conversations private." (Defendants' brief on appeal at 32.) They assert that

the district court's fundamental error stems from its assumption that a recording that is destroyed without being heard violates privacy interests to the same extent and in the [**39] same manner as a recording this is listened to.

(Id. at 33 (emphasis added).) Similarly, while apparently acknowledging the clarity of the Fifth Amendment's guarantee of the arrestee's right to remain silent, right to consult an attorney prior to any police interrogation, and right not to have evidence obtained in violation of those rights used against the him (see, e.g., id. at 32, 34), defendants argue that the rejection of their immunity defense with respect to the Fifth Amendment claims was erroneous because

the court apparently equated unheard recordings with interrogation, although it should be obvious that a conversation that is recorded but destroyed without being heard cannot provide any information that could be considered "a link in the chain of evidence that could lead to prosecution."

(Id. at 34 n.22 (emphases added).) And defendants argue that all of the authorities discussed by the district court in addressing plaintiffs' claims under the Fourth Amendment and Title III are distinguishable from the present case because those cases dealt with recordings that had been listened to. See, e.g., Katz v. United States, [**40] 389 U.S. 347, 353, 19 L. Ed. 2d 576, 88 S. Ct. 507 (1967) (government's "electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied . . . and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment" (emphasis added)); United States v. Turk, 526 F.2d 654, 658 n.3 (5th Cir.) ("If . . . the recording is made, but is destroyed before anyone can hear it, whether there has been an 'aural acquisition' [within the meaning of Title III] is a nice question."), cert. denied, 429 U.S. 823, 50 L. Ed. 2d 84, 97 S. Ct. 74 (1976).

Thus, every argument made to us by defendants in support of their qualified-immunity defense depends on their contention that there was no listening to confidential conversations. That, however, is a factual contention that defendants have not established. It is no answer to say, as defendants do, that plaintiffs have produced no specific evidence of listening or use, for on this motion for summary judgment, plaintiffs do not have the burden of proof. To the extent that plaintiffs do have a burden to come forward with sufficient evidence to show a genuine issue to be tried, there is in the record ample evidence that there was State [**41] Police listening to at least some recorded conversations. For example, defendant John Bardelli was commanding officer of one troop; and for a

time during the period in question, he had responsibility for inspecting the taping systems in all of the barracks. In the latter capacity, Bardelli conducted detailed inspections and routinely instructed a sergeant to select a tape at random, take it to State Police headquarters, and spend a full day listening to conversations on it. Though Bardelli testified that the intent was not to listen to confidential conversations, he acknowledged that the sergeant had access to every conversation on the tape. Since "it is undisputed that the State Police's recorders did not possess the capability to locate a particular call automatically," 888 F. Supp. at 1263, that they [*126] "did not distinguish between incoming and outgoing calls," *id.* at 1242, and that there was no way to tell, without listening, where a given call ended, a rational factfinder could infer that the listening officer would routinely have heard conversations other than those he was entitled to hear, including confidential conversations in outgoing calls made by arrestees.

Bardelli also [**42] testified that, with respect to the period in which he was a troop commander, he could not say that all of the recorded telephones in the barracks he commanded bore warning labels; he did not recall whether stickers were placed on telephones in the holding room to indicate taping; he did not know of any warning signs in the holding room to indicate that some lines were recorded; and he did no monitoring to ensure that arrestees had access to an unrecorded line.

There is also evidence from which a rational factfinder could infer that recorded confidential conversations were used against arrestees. For example, Bardelli testified that he was aware that some requests for particular recorded conversations had been received from State's Attorneys. And though defendants state that tapes were routinely erased within 60 days, the tapes of the attorney-client conversations at issue in Ferrell remained available some three years after they were made, and the prosecution used them in an attempt to establish that Ferrell had no reasonable expectation of privacy in his statements to his attorneys.

Thus, the record includes evidence from which it could be inferred not only that arrestees had [**43] no notice that conversations they expected to be confidential were being recorded, but also that confidential conversations were listened to and used in criminal investigations. Viewed in the light most favorable to plaintiffs as the parties opposing summary judgment, the record more than suffices to show genuine issues of fact to be tried as to, *inter alia*, whether there was listening to, disclosure of, and use of confidential conversations, as plaintiffs have maintained.

In light of these factual issues, the policy considerations underlying the immediate appealability of a denial of summary judgment based on a determination of legal issues, set out in *Mitchell* and adumbrated in *Johnson v. Jones*, are not served by an immediate appeal. The qualified-immunity defense asserted here depends on the resolution of defendants' factual premise that there was no listening to recorded confidential conversations; if the factfinder finds such listening, the qualified-immunity defense will be mooted, for defendants do not contend that they have immunity if there was listening; if the factfinder concludes that there was no such listening but finds in favor of plaintiffs nevertheless, [**44] the qualified-immunity defense can be determined at that point. The postponement of consideration of defendants' immunity defense until after trial does not deprive defendants of an opportunity to avoid a trial, for the nature of their defense affords them no such opportunity: recording is conceded, and the immunity defense asserted here cannot be resolved without a trial to determine, *inter alia*, whether there was listening, to what extent there was listening, and whether there was use. Thus, though the qualified-immunity defense is meant to protect defendant officials from going to trial, that defense as asserted here, even if upheld, can have no such effect, for an appellate opinion in favor of either party on the hypothetical legal question posed by defendants would not eliminate the need for a trial on any claim.

B. State-Law Immunity

For similar reasons, we conclude that the district court's denial of summary judgment with respect to defendants' defense of qualified immunity as to plaintiffs' state-law claims is unappealable. The Connecticut eavesdropping statute expressly prohibits the "intentional overhearing or recording of a telephonic . . . communication," [**45] Conn. Gen. Stat. § 53a-187(a)(1) (1994) (emphasis added); see also *id.* § 54-41a(2) (Wiretap Act) ("Intercept" means the intentional overhearing or

recording of a wire communication through the use of any electronic, mechanical or other device." (emphasis added)). Thus, at the time that Connecticut used its taping system, defendants knew or should have known that they were violating rights [*127] that were clearly established under state statutory law.

Under Connecticut law, state officials do not have immunity for such violations if, inter alia, their actions were likely to subject an identifiable person to imminent harm or if their alleged misconduct involved malice, wantonness, or the intent to injure. See Evon v. Andrews, 211 Conn. at 505, 559 A.2d at 1134. The district court ruled that there were factual questions to be tried as to these immunity issues. That ruling is not appealable.

CONCLUSION

In sum, the district court in denying defendants' qualified-immunity-based motion for summary judgment, found that there were genuine issues of fact to be tried as to, inter alia, whether plaintiffs expected their telephone conversations to be confidential, see, [**46] e.g., 888 F. Supp. at 1258, 1261; whether defendants gave telephone users notice of the recording sufficient to make any such expectation of privacy unreasonable, see, e.g., id. at 1258, 1259, 1261, 1265, 1266; whether and to what extent defendants listened to tapes of confidential conversations, see, e.g., id. at 1263-64, 1267, 1270-71; and whether such conversations were "used" in violation of plaintiffs' Fifth Amendment rights, see, e.g., id. at 1257. The availability of qualified immunity depends on the resolution of these fact issues. This is not an appropriate case for an immediate appeal of the denial of defendants' motion for summary judgment.

At trial, the district court should submit to the jury special interrogatories the answers to which will disclose whether any verdict in favor of a plaintiff is based on conversations that were recorded but not used or listened to.

We have considered all of defendants' arguments in support of appealability and have found them to be without merit. The appeal is dismissed for lack of appellate jurisdiction.

View: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)

[FOCUS™ - Narrow Results](#) | [More Like This](#) | [More Like Selected Text](#) | [Shepardize®](#)

In re **STATE**, 88 F.3d 111

Topic: [All Topics](#) : [Criminal Law & Procedure](#) : [Search & Seizure](#) : **[Expectation of Privacy - US Courts of Appeals Cases - All Circuits - Selected Criminal Material](#)**

Terms: **wire tapping** ([Edit Search](#))

View: Full

Date/Time: Wednesday, July 5, 2000 - 4:34 PM EDT

[Search](#) | [Search Advisor](#) | [Get a Document](#) | [Check a Citation](#)
[ECLIPSE\(TM\)](#) | [History](#) | [Change Client](#) | [Options](#) | [Feedback](#) | [Sign Off](#) | [Help](#)
[About LEXIS-NEXIS](#) | [Terms and Conditions](#)

Copyright © 2000 LEXIS-NEXIS Group. All rights reserved.

lexis.com™

[Change Client](#) [Options](#) [Feedback](#) [Sign Off](#) [Help](#)[Search](#) [Search Advisor](#) [Get a Document](#) [Check a Citation](#)[ECLIPSE™](#) [History](#)View: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#)[PREVIOUS](#) 3 of 11 [NEXT](#)[Text Only](#) | [Download](#) | [Fax](#) | [Email](#)[FOCUS™](#) - [Narrow Results](#) | [More Like This](#) | [More Like Selected Text](#) | [Shepardize®](#)**UNITED STATES v. PETERSON, 812 F.2d 486**Topic: [All Topics](#) : [Criminal Law & Procedure](#) : [Search & Seizure](#) : **Expectation of Privacy - US Courts of Appeals Cases**
- **All Circuits - Selected Criminal Material**Terms: **wire tapping** ([Edit Search](#))*812 F.2d 486, *; 1987 U.S. App. LEXIS 3125, ***UNITED STATES OF AMERICA, Plaintiff-Appellee v. TIMOTHY NICHOLAS PETERSON, DARRYL RAY
HOOD, STEPHEN ALLEN FALK, and PAUL JULES GOUDEAU, Defendants-Appellants

Nos. 85-5167, 85-5168, 85-5173, 85-5174

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

812 F.2d 486; 1987 U.S. App. LEXIS 3125

May 9, 1986, Argued and Submitted
March 9, 1987, Filed**PRIOR HISTORY:**

[**1] Appeal from the United States District Court for the Southern District of California, Howard B. Turrentine, Senior District Judge, Presiding, D.C. Nos. 85-0040-01-T, 85-0040-04-T, 85-0040-02-T, 85-0040-03-T.

DISPOSITION: The judgment of the district court is AFFIRMED.**CORE TERMS:** wiretap, ship, marijuana, vessel, apartment, waters, high seas, seizure, crew, customs, statutory authority, exclusionary rule, boarding, foreign law, transmission, certificate, radio, international law, distribute, public safety, authorization, confirmation, telephone, message, seized, law enforcement, joint venture, extraterritorial, conditional, deposition**COUNSEL:** Ephraim Margolin, Victor Sherman, and Juanita R. Brooks, for the Plaintiff-Appellant.

Roger Haines, Assistant United States Attorney, for the Defendant-Appellee.

JUDGES: James R. Browning, Anthony M. Kennedy and Robert R. Beezer, Circuit Judges.**OPINIONBY:** KENNEDY**OPINION:** [*488] KENNEDY, Circuit Judge:

Appellants appeal their convictions for possession of a controlled substance (marijuana) in the United States customs waters with the intent to distribute and for conspiracy to destroy goods to prevent seizure, in violation of 18 U.S.C. § 2 and 21 U.S.C. § 955a(c), and 18 U.S.C. §§ 371, 2232. Following denial of their motions to suppress evidence, appellants entered conditional guilty pleas on the possession charge. The parties submitted the conspiracy charge to the district court on a set of stipulated facts, and the trial court convicted.

In early 1984, the Bangkok office of the Drug Enforcement Agency (DEA) learned from a confidential informant of a plan to smuggle thirty-two tons of a marijuana [**2] from Thailand. The DEA

identified appellant Falk as a participant and notified Thai authorities of his presence in that country. In Bangkok, Thai narcotics authorities wiretapped telephones in Falk's rented apartment, and at a government post office where appellant Peterson made calls. The Thai officials provided information from the wiretaps to the DEA, and, since the tapes were in English, the DEA translated some of them.

The DEA and Thai authorities learned that a ship, the *Allyson*, was leaving Thailand for the West Coast of the United States. The *Allyson* stopped in Manila for repairs and then departed, though the Manila office of the DEA and Philippine authorities had been notified of the investigation. Later, the DEA seized the ship in Alaska and found approximately twelve tons of marijuana on board.

The DEA learned that the same persons who arranged for the *Allyson* shipment would use another vessel, the *Pacific Star*, for a second marijuana shipment from Thailand. The DEA found that the *Pacific Star* was en route to the Philippines and notified Philippine authorities. The Philippine Narcotics Command (NARCOM) commenced surveillance on an associate of Falk who [**3] resided at an apartment in Manila. NARCOM discovered a tri-band radio transmitter was operating illegally from the apartment and began monitoring and taping the radio transmissions between the apartment and the *Pacific Star*. The frequencies had been obtained from the DEA, and, as many of the transmissions were in code, the DEA deciphered them. Between November 29, 1984, and December 10, 1984, Philippine authorities tapped the telephone [*489] in the apartment and provided the DEA with tapes of those interceptions as well. In one of the calls intercepted by the telephone tap, someone talking from the United States referred to "100 south of Cabo."

The United States Coast Guard cutter *Citrus* was engaged to intercept the *Pacific Star* and found it as it headed to a position one hundred miles south of Cabo San Lucas. Lieutenant Commander Giraitis contacted the *Pacific Star* by radio and requested the ship's registration, identification, and travel itinerary. The radio operator on board the *Pacific Star* responded that the ship was Panamanian, had departed the Philippines nonstop for Panama, and was experiencing mechanical difficulties. Giraitis noted that it was unusual for a [**4] ship as small as the *Pacific Star* to travel such a long distance nonstop.

Giraitis informed the radio operator on board the *Pacific Star* that he was going to verify the ship's registration with Panamanian authorities and seek permission to come on board, unless the *Pacific Star* would consent to his boarding. Consent was refused. A DEA special agent contacted a Panamanian official concerned with narcotics enforcement and obtained authority for the Coast Guard to search the *Pacific Star* in the name of the Panamanian government; no formal written authorization was obtained at that time. The next morning Giraitis informed the *Pacific Star* that a party would board the ship. The ship did not stop, and its crew set it on fire. As the Coast Guard boarded the *Pacific Star*, that ship rammed the *Citrus*. The *Pacific Star* sank, and the Coast Guard recovered the marijuana. The *Pacific Star* crew jettisoned some marijuana and the Coast Guard recovered it as well.

The principal contention, here and in the district court, has been that the marijuana is inadmissible because unlawfully seized. The bases for appellants' evidentiary challenge are: that discovery of the [**5] ship and its contraband is tainted by unlawful wiretaps participated in by United States officials; that the boarding was without statutory authority in any event, among other reasons because the consent of Panama was required and not obtained; and that the search was unlawful because no warrant was obtained. These contentions are unavailing, in part because the factual premises are incorrect and in part because the legal premises are wrong. We explain in further detail.

While neither the Supreme Court nor this Court has stated definitively the extent to which fourth amendment protections apply upon the high seas, it has been assumed to apply in our major decisions. See, e.g., *United States v. Troise*, 796 F.2d 310 (9th Cir. 1986); *United States v. Cilley*, 785 F.2d 651 (9th Cir. 1985); *United States v. Watson*, 678 F.2d 765 (9th Cir.), cert. denied, 459 U.S. 1038, 74 L. Ed. 2d 605, 103 S. Ct. 451 (1982). The government makes the same assumption here, so the case is presented as one in which the fourth amendment is applicable. Because there are

multiple, and abundant, grounds for sustaining the actions of the Coast Guard, this is not an appropriate decision to delineate the outer limits of the Coast Guard's [**6] authority to stop and board on the high seas and then to search below decks.

We begin by considering whether the Philippine wiretap tainted the stop of the vessel and the subsequent discovery of the contraband. The government does not argue that the suspicious behavior of the *Pacific Star* and its crew, the crew's actions in setting it on fire, the ramming of the *Citrus*, or jettisoning of the cargo were independent criminal acts so attenuated from the wiretap that the taint is broken; and as the record is somewhat unclear respecting the sequence of these events, we treat the case as one in which suppression of this evidence would be required if evidence from the wiretap itself is inadmissible. We conclude that evidence from the wiretap is not subject to the exclusionary rule under the circumstances of this case.

The appellants invite us to consider the possibility that the evidence is the fruit of illegal wiretaps not only in the Philippines, but also in Thailand. We disagree. The wiretaps in Thailand led the DEA to the seizure of the *Allyson*, not the *Pacific* [*490] *Star*. A confidential informant, not the wiretaps, alerted the DEA that the *Pacific Star* would be in the [**7] Philippines. The chain of any taint from the Thai wiretaps was broken. *Cf. Wong Sun v. United States*, 371 U.S. 471, 491 (1963).

Appellants suggest that the interception of radio transmissions between the apartment in Manila and the *Pacific Star* was an illegal search. This conclusion is untenable. The broadcasts took place on channels in open use, most often by fishermen. The appellants had no legitimate expectation of privacy in the radio communications. *United States v. Rose*, 669 F.2d 23, 25 (1st Cir.) (no privacy expectations in radio transmission because not "objectively reasonable"), *cert. denied*, 459 U.S. 828, 103 S. Ct. 63, 74 L. Ed. 2d 65 (1982). The evidence derived from the radio transmissions was not obtained illegally.

These contentions aside, the point reduces to whether the Philippine wiretap, which allowed authorities to locate the *Pacific Star*, was an illegal search. The government maintains the appellants lack standing to assert that wiretap was illegal, and the district court so held. We conclude, however, that at least one of four appellants has standing to contest its legality.

Appellant Falk declared that he "resided in" the Manila apartment from September 1984 to December 31, [**8] 1984. He said also he was a sublessee of the apartment. Although the government had a chance to cross-examine Falk on these matters, it chose not to do so. Falk's assertions in the affidavit are uncontradicted and establish a possessory interest in the apartment sufficient to confer standing. *Alderman v. United States*, 394 U.S. 165, 176, 22 L. Ed. 2d 176, 89 S. Ct. 961 (1969). Our conclusion that Falk had standing requires us to reach the substance of appellants' various claims. In light of our ultimate resolution of these claims, we need not decide whether any of the other appellants standing.

We must address whether agents of the United States had sufficient participation in the wiretaps to invoke exclusionary rule analysis. With certain exceptions not applicable here, fourth amendment principles do not apply to searches by foreign authorities in their own countries, even if the targets of the search are American. *United States v. Rose*, 570 F.2d 1358, 1361 (9th Cir. 1978). If, however, United States agents' participation in the investigation is so substantial that the action is a joint venture between United States and foreign officials, the law of the foreign country must be consulted at the outset as part [**9] of the determination whether or not the search was reasonable.

The district court concluded that no joint venture existed between United States and Philippine authorities. United States agents, however, termed their actions a "joint investigation" in their own testimony. The DEA was involved daily in translating and decoding intercepted transmissions, as well as advising the Philippine authorities of their relevance. The DEA treated the affair as one in which the marijuana was destined for the United States, and so assumed a substantial role in the case. In all of the circumstances here, we are unable to conclude that the DEA's role was subordinate to the role of Philippine authorities. *Cf. Stonehill v. United States*, 405 F.2d 738, 746 (9th Cir. 1968), *cert. denied*, 395 U.S. 960, 89 S. Ct. 2102, 23 L. Ed. 2d 747 (1969). The district judge erred in concluding

that the operation was not a joint venture.

The propriety of the wiretaps under principles of Philippine law presents a more difficult question. The district court found that there was an insufficient showing to establish a violation of Philippine law. Foreign law, though formerly treated as an issue of fact, is now recognized as an issue of law, to be [**10] established by any relevant source, including testimony. Fed. R. Crim. P. 26.1; Fed. R. Civ. P. 44.1. As an appellate court, we are able to determine the relevant legal standards. See Miller, *Federal Rule 44.1 and the "Fact" Approach to Determining Foreign Law: Death [**491] Knell for a Die-Hard Doctrine*, 65 Mich. L. rev. 613, 689-91 (1967) (appellate courts should be free to examine foreign law questions on appeal). At our request, the parties filed supplemental briefs on the question.

Two provisions of Philippine law control the inquiry, the first being article IV, section 4, of the Philippine Constitution. The section provides: "(1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety and order require otherwise. (2) Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding." The second law is provided by Republic Act 4200, Philippine Permanent and General Statutes, Trinidad, Ed. (Quezon City 1978):

It shall be unlawful . . . to tap any wire or cable. . . .

Nothing contained in this Act, however, shall render it unlawful or punishable [**11] for any peace officer, who is authorized by a written order of the Court, to [wiretap] in cases involving the crimes of treason, espionage, provoking war and disloyalty in case of war, piracy, mutiny in the high seas, rebellion, conspiracy and proposal to commit rebellion, inciting rebellion, sedition, conspiracy to commit sedition, kidnapping as defined by the Revised Penal Code, and violations of Commonwealth Act No. 616, punishing espionage and other offenses against national security: *Provided*, That such written order shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce. . . .

All concede judicial authorization was neither sought nor received. This, the appellants argue, should decide the issue, and they cite a student note for the proposition that may wiretap not complying with the judicial authorization procedures of Act 4200 is illegal. See Note, *The Wire Tapping Law and Its Constitutional Implications*, 41 Philippine L.J. 352 (1966). The government argues, however, that the statute does not delimit all permissible wiretaps. It contends Act 4200 merely implements the [**12] "lawful order of the court" exception to the wiretapping prohibition of article IV, section 4, of the constitution, and that there still remains the further exception for "public safety and order" concerns. We agree. See E. Fernando, *The Constitution of the Philippines* 661-62 (2d ed. 1977). The government also points out that a presidential executive order, signed November 16, 1972, and since repealed, made it illegal for anyone to wiretap *unless* that person complied with Act 4200. Presidential Decree No. 55, Penalizing Unauthorized Telephone Installations, Philippine Permanent and General Statutes, Trinidad, Ed. (Quezon City 1984) (repealed 1981). This decree would have been unnecessary if Act 4200 was the exclusive source of exceptions to the prohibition on wiretapping.

We have found no Philippine court decision interpreting the scope of the public safety exception in article IV, section 4, and we have little guidance in determining whether the wiretap here, an interception intended to interdict a major drug ring, would fall within the clause. Philippine courts have a long history of construing their constitution in favor of individual liberties. See, e.g., *Marcelo v. De Guzman*, [**13] 114 Philippine Sup. Ct. Reports Ann. 657 (1982); see also *id.* at 664 (Aquino, J., concurring) (holding that evidence seized pursuant to an insufficiently particular warrant must be excluded). We conclude it is plausible that the term public safety is intended for grave threats directed to the security of the state or its people, not for a discrete transaction to distribute

drugs outside the Philippines. We will assume the correctness of this view for analytic purposes. We decide the case on the assumption that the search did not comply with Philippine law and was, as a result, not reasonable under the fourth amendment.

Although local law of the Philippines governs whether the search was reasonable, our law governs whether illegally obtained evidence should be excluded, and the essence of our inquiry is whether exclusion serves the rationale of deterring federal officers from unlawful conduct. At this [*492] point, the good faith exception to the exclusionary rule becomes part of the analysis. See United States v. Leon, 468 U.S. 897, 82 L. Ed. 2d 677, 104 S. Ct. 3405 (1984). The determination whether federal officers will be deterred by the exclusion of evidence in a federal courtroom is a decision that necessarily [**14] implicates federal interests, and federal law determines whether the exclusionary remedy should be invoked.

The good faith exception is grounded in the realization that the exclusionary rule does not function as a deterrent in cases in which the law enforcement officers acted on a reasonable belief that their conduct was legal. It is true, as appellants note, that *Leon* speaks only in terms of good faith reliance on a facially valid search warrant. That is not dispositive, however. We conclude that the reasoning applies as well to reliance on foreign law enforcement officers' representations that there has been compliance with their own law. See also Massachusetts v. Sheppard, 468 U.S. 981, 989-90, 82 L. Ed. 2d 737, 104 S. Ct. 3424 (1984) (holding that officers were entitled to rely on a magistrate's representations that all necessary changes to the form of the warrant would be made). American law enforcement officers were not in an advantageous position to judge whether the search was lawful, as would have been the case in a domestic setting. Holding them to a strict liability standard for failings of their foreign associates would be even more incongruous than holding law enforcement officials to a strict [**15] liability standard as to the adequacy of domestic warrants. We conclude that the good faith exception to the exclusionary rule announced in *Leon* applies to the foreign search.

We do not suggest that objectively unreasonable reliance on foreign law officers can cloak the search with immunity from the exclusionary rule. That said, permitting reasonable reliance on representations about foreign law is a rational accommodation to the exigencies of foreign investigations. The reliance in this case was objectively reasonable. A review of the record reveals that the federal officers sought, and received, assurances from high ranking law enforcement authorities in the Philippines that all necessary authorization was being obtained. As our discussion above may indicate, search and seizure law in the Philippines is less than completely clear. We hold that the seized marijuana, and other evidence on the *Pacific Star*, was admitted properly against the appellees' fourth amendment objection to the Philippine wiretap.

Appellants also argue that the wiretap [**16] evidence should be excluded as violative of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20 (1982). We reject this argument. Title III has no extraterritorial force. Stowe v. Devoy, 588 F.2d 336, 341 n.12 (2nd Cir. 1978) United States v. Cotroni, 527 F.2d 708, 711 (2d Cir. 1975), cert. denied, 426 U.S. 906, 96 S. Ct. 2226, 48 L. Ed. 2d 830 (1976).

The question whether boarding the *Pacific Star* violated appellants' rights under international law need not detain us. appellants claim that the seizure of the ship was in violation of article 6 of the Convention on the High Seas, opened for signature, Apr. 29, 1958, 13 U.S.T. 2312, T.I.A.S. No. 5200, 450 U.N.T.S. 82 (entered into force Sept. 30, 1962). The ramifications of a violation of international law are largely political, and any violation of international law here is relevant only as it informs our decision on whether the search was or was not in violation of our statutory and constitutional standards. The treaty is not self-executing in the sense that it confers individual rights on these litigants to suppress evidence. If the search was properly authorized, a violation of the treaty would not allow for exclusion of the evidence. [**17] See United States v. Williams, 617 F.2d 1063, 1089-90 (5th Cir. 1980). In any event, as we discuss below, Panama's consent removes international law concerns from the case. *Id.*

The statutory authority of the Coast Guard to stop and board the vessel is the next subject of

discussion. The underlying assumption that absence of statutory authority would require suppression of the [*493] evidence need not be explored, for we find that the Coast Guard had statutory authority for its actions.

The Coast Guard was acting within its statutory authority in boarding the ship. 14 U.S.C. § 89(a) provides, in part, as follows:

The Coast Guard may make inquiries, examinations, inspections, searches, seizures, and arrests upon the high seas and waters over which the United States has jurisdiction, for the prevention, detection, and suppression of violations of laws of the United States. For such purposes, commissioned, warrant, and petty officers may at any time go on board of any vessel subject to the jurisdiction, or to the operation of any law, of the United States, address inquiries to those on board, examine the ship's documents and papers, and examine, inspect, and search the vessel and use [**18] all necessary force to compel compliance.

21 U.S.C. § 955a(c) makes it illegal to knowingly manufacture, distribute, or possess with the intent to manufacture or distribute controlled substances, while in the customs waters of the United States. The statute specifically applies to the high seas and does not restrict the Coast Guard to actions based on reasonable suspicion or probable cause. It has been held in the Fifth Circuit that reasonable suspicion is required if the Coast Guard chooses to rely on the jurisdictional predicate that a foreign vessel is operating in violation of American laws. Williams, 617 F.2d at 1076. In the instant case, however, the statutory basis for asserting jurisdiction over the vessel is that it was boarded within the customs waters of the United States.

The *Pacific Star* was within such waters. 21 U.S.C. § 955 (a) points to 19 U.S.C. § 1401(j) to define "customs waters"; this definition is also found in 19 U.S.C. § 1709(c). Section 1709(c) enacts that customs waters can be extended beyond the normal limit of one hour's sailing time, provided there exists an arrangement between the United States and the foreign country.

Panama and the Coast Guard [**19] arranged for the Coast Guard to board the ship. The telex message that the Coast Guard received read: "GOVT OF PANAMA HAS AUTHORIZED U.S. COAST GUARD TO BOARD, SEARCH AND SEIZURE SUBJ VESSEL ON THEIR BEHALF IF EVIDENCE WARRANTS THIS ACTION." Appellants argue that the arrangement was merely conditional, and that, fairly read, it does not give authority to board. While it is true that the message is conditional, the conditions were satisfied. The Coast Guard had evidence to justify the boarding; and the message required no more.

Appellants argue that the proper authorization procedures were not followed in obtaining the consent. A foreign service officer, however, testified that the Panamanian inspector, directly responsible for the authorization, did in fact have the power to give authority to the Coast Guard to board ships. The testimony also indicated that the procedure does not involve a warrant. Other courts have admitted teletype messages in lieu of warrants. See, e.g., United States v. Loalza-Vasquez, 735 F.2d 153, 157-58 (5th Cir. 1984); see also United States v. Gonzalez, 776 F.2d 931, 935-37 (11th Cir. 1985) (telephone authorization sufficient). This was sufficient [**20] to extend the customs waters of the United States.

We also reject appellants' argument that section 955a, so construed, is an improper and unconstitutional exercise of extraterritorial jurisdiction. We conclude that there was more than a sufficient nexus with the United States to allow the exercise of jurisdiction. There was substantial evidence that the drugs were bound ultimately for the United States. Where an attempted transaction is aimed at causing criminal acts within the United States, there is a sufficient basis for the United States to exercise its jurisdiction to arrest and try the offenders. See, e.g., United States v. Baker, 609 F.2d 134 (5th Cir. 1980). Further, drug trafficking may be prevented under the

protective principle of jurisdiction, without any showing of an actual effect on the United States. United [*494] States v. Pizzarusso, 388 F.2d 8, 10-11 (2d Cir.), cert. denied, 392 U.S. 936, 88 S. Ct. 2306, 20 L. Ed. 2d 1395 (1968). Protective jurisdiction is proper if the activity threatens the security or governmental functions of the United States. Restatement Second of Foreign Relations § 33. Drug trafficking presents the sort of threat to our nation's ability [**21] to function that merits application of the protective principle of jurisdiction. Cf. United States v. Marino-Garcia, 679 F.2d 1373, 1378 n.4 (11th Cir. 1982), cert. denied, 459 U.S. 1114, 74 L. Ed. 2d 967, 103 S. Ct. 748 (1983). Accordingly, we conclude that jurisdiction was properly exercised over the appellants.

In concluding that the cited statutes properly authorize the search, we do not hold that statutes are the exclusive source of the Coast Guard's power to stop, board, and seize ships. There may be other sources of governmental power that would authorize a stop. United States v. Ramsey, 431 U.S. 606, 615, 52 L. Ed. 2d 617, 97 S. Ct. 1972 (1977) (executive authority is a possible source of permissible searches); Williams, 617 F.2d at 1074 ("Ramsey indicates that the source of authority for a seizure or search need not be statutory. . ."). In this case, however, the search was authorized statutorily, and we need not consider the availability of other sources.

The question we next face is whether the search violated the fourth amendment, which, as we have stated earlier, is here assumed [**22] to be applicable.

The appellants argue that whatever the statutory authority to board, the fourth amendment prohibited the search and seizure that followed. There is much imprecision as to what search took place and what was seized as a result of it. The vessel itself sank despite the Coast Guard's efforts to save it; the crew was arrested for criminal acts which occurred on the scene as well as for violations of the drug laws; and, apparently, some marijuana was jettisoned and some floated from the hold as the ship sank. We would be justified in rejecting appellants' claims for such lack of specificity, particularly as it prevents us from applying rules of standing which again come into play, it being well settled that the crew has no legitimate expectation of privacy in the cargo hold of a vessel. United States v. Pinto-Mejia, 720 F.2d 248, 255 (2d Cir. 1983), modified on other grounds, 728 F.2d 142 (2d Cir. 1984). We need not rest our conclusions on this basis, however. Assuming that this was a stop and a search for criminal violations at the outset, and that fourth amendment protections are fully applicable, a point that is far from settled, there was probable cause to [**23] search and seize the vessel, its cargo, and its crew. Searches of vessels on the high seas in such circumstances may be warrantless, as the location of the vessels and the practical difficulties of obtaining a warrant while at sea present exigent circumstances under well accepted principles. United States v. Cilley, 785 F.2d 651, 653-55 (9th Cir. 1985); United States v. Maybusher, 735 F.2d 366, 372 (9th Cir. 1984), cert. denied, 469 U.S. 1110, 83 L. Ed. 2d 783, 105 S. Ct. 790 (1985). We find, therefore, no constitutional or other invalidity in the stop, the board, the search, or the seizure of the evidence in this case.

Appellant Falk raises the question whether the district court should have granted his motion for leave to take the deposition of four Americans and two Panamanians, all located in Panama, in order for Falk to ascertain the validity of Panama's consent to the Coast Guard's boarding. The district court denied the taking of the depositions but ordered subpoenas for two of the Americans. This matter is within a district court's discretion. Furlow v. United States, 644 F.2d 764, 767 (9th Cir.), cert. denied, 454 U.S. 871, 70 L. Ed. 2d 175, 102 S. Ct. 340 (1981). Falk made no showing that the other four witnesses would [**24] submit to oral depositions, or that their testimony would not be cumulative of the other two witnesses.

We next decide whether the district court improperly admitted into evidence, at a pretrial hearing, an exhibit containing: (1) a letter from the United States embassy in Panama requesting written confirmation of Panamanian consent to board the *Pacific [*495] Star*, and (2) a certificate, indicating written confirmation, from the Director General of the Consular and Shipping Affairs Section of Panamanian Ministry of Finance and Treasury. The exhibit was admitted for its truth, and is therefore hearsay.

Appellants argue that the exhibit did not possess sufficient "circumstantial guarantees of

trustworthiness" to be admissible under Federal Rule of Evidence 803(24). Appellants point out that the Panamanian certificate was dated three weeks after the seizure. The certificate also stated that it was "at the request of the United States Embassy." The embassy letter, purporting to request the certificate, was dated one month *after* the date on the certificate. We do not believe, however, that the district judge abused his discretion in admitting the exhibit. United States v. Burreson, [****25**] 643 F.2d 1344, 1349 (9th Cir.), *cert. denied*, 454 U.S. 847, 70 L. Ed. 2d 135, 102 S. Ct. 165 (1981). An embassy official testified that, because the embassy regularly requests confirmation, the confirmation was prepared ahead of time. In any event, even without the document, there was substantial evidence of Panamanian consent, most notably the telex sent to the Coast Guard.

We finally consider whether there was sufficient evidence to convict the appellants of conspiracy to destroy property, i.e. the marijuana, in violation of 18 U.S.C. § 2232. Appellant Peterson contends, without any citation, that section 2322 does not have any extraterritorial reach. However, since section 2322 proscribes conduct related to section 955a, we think it untenable that Congress did not intend a similar reach.

In reviewing the sufficiency of the evidence to sustain a conviction, "the relevant question is whether, after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." Jackson v. Virginia, 443 U.S. 307, 319, 61 L. Ed. 2d 560, 99 S. Ct. 2781 (1979) (emphasis in original). The answer to this question, in this case, is "yes." The evidence [****26**] shows that the marijuana was thrown overboard from the *Pacific Star*, and that the ship was set on fire. Under these circumstances, a rational trier of fact could have found a violation of section 2322 beyond a reasonable doubt.

The judgment of the district court is AFFIRMED.

View: [Cite](#) | [KWIC](#) | [Full](#) | [Custom](#) | [PREVIOUS](#) 3 of 11 [NEXT](#) | [Text Only](#) | [Download](#) | [Fax](#) | [Email](#)
[FOCUS™](#) - [Narrow Results](#) | [More Like This](#) | [More Like Selected Text](#) | [Shepardize®](#)

UNITED STATES v. PETERSON, 812 F.2d 486

Topic: [All Topics](#) : [Criminal Law & Procedure](#) : [Search & Seizure](#) : [Expectation of Privacy - US Courts of Appeals Cases - All Circuits - Selected Criminal Material](#)

Terms: **wire tapping** ([Edit Search](#))

View: Full

Date/Time: Wednesday, July 5, 2000 - 4:35 PM EDT

[Search](#) | [Search Advisor](#) | [Get a Document](#) | [Check a Citation](#)
[ECLIPSE\(TM\)](#) | [History](#) | [Change Client](#) | [Options](#) | [Feedback](#) | [Sign Off](#) | [Help](#)
[About LEXIS-NEXIS](#) | [Terms and Conditions](#)

Copyright © 2000 LEXIS-NEXIS Group. All rights reserved.