

* Canton Sedgely

GW
GEORGETOWN
AMERICAN *
PENN
STANFORD

202-885-1800

PHOTOCOPY
PRESERVATION

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

Draft 07/12/00 11:35am

Gottheimer/ Swire

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

This week millions of Americans are waiting in line to buy a hotly anticipated book. No it's not Harry Potter. *[hold up book]* It's actually *Protecting Electronic Messaging* by John Podesta -- a book I wrote when I was on the Hill a few years ago. I'll be signing copies after the speech. Buy one for each of your children.

Today I want to return to some of the topics from my not-quite best-selling book -- particularly the issue of how to protect privacy and civil liberties, while also protecting public safety in an electronic age.

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

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn't even imagined just a few years before.

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

Today, the great revolution in communication technology continues. From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a remarkable reservoir of information -- from Shakespeare's first sonnet to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values -- and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information -- from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has worked to build a framework for trust and security in this new world of electronic networks. We've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And to combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. This February, in his Cyber Security Summit, the President emphasized the primary role and responsibility of the private sector in ensuring computer and network security. As you know, most computers and networks that we rely upon every day are owned and operated by the private sector. It's only right that they -- not the government -- take the leading role in making security a standard part of the Internet.

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

Today we are taking a significant new step to update our export controls. Under new government regulations, we're taking down the barriers that prevent corporations from exporting encryption to governments and businesses in the European Union and eight other trading partners. We're also speeding up the time-to-market, by eliminating the thirty-day waiting period for exporting encryption goods.

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 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 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.

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.

[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, 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 11:35am

Gottheimer/ Swire

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

This week millions of Americans are waiting in line to buy a hotly anticipated book. No it's not Harry Potter. *[hold up book]* It's actually *Protecting Electronic Messaging* by John Podesta -- a book I wrote when I was on the Hill a few years ago. I'll be signing copies after the speech. Buy one for each of your children.

Today I want to return to some of the topics from my not-quite best-selling book -- particularly the issue of how to protect privacy and civil liberties, while also protecting public safety in an electronic age.

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

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn't even imagined just a few years before.

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

Today, the great revolution in communication technology continues. From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a remarkable reservoir of information -- from Shakespeare's first sonnet to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values -- and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information -- from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has worked to build a framework for trust and security in this new world of electronic networks. We've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And to combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. This February, in his Cyber Security Summit, the President emphasized the primary role and responsibility of the private sector in ensuring computer and network security. As you know, most computers and networks that we rely upon every day are owned and operated by the private sector. It's only right that they -- not the government -- take the leading role in making security a standard part of the Internet.

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

Today we are taking a significant new step to update our export controls. Under new government regulations, we're taking down the barriers that prevent corporations from exporting encryption to governments and businesses in the European Union and eight other trading partners. We're also speeding up the time-to-market, by eliminating the thirty-day waiting period for exporting encryption goods.

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 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 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.

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.

[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, 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 11:35am
Gottheimer/ Swire

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

This week millions of Americans are waiting in line to buy a hotly anticipated book. No it's not Harry Potter. *[hold up book]* It's actually *Protecting Electronic Messaging* by John Podesta -- a book I wrote when I was on the Hill a few years ago. I'll be signing copies after the speech. Buy one for each of your children.

Today I want to return to some of the topics from my not-quite best-selling book -- particularly the issue of how to protect privacy and civil liberties, while also protecting public safety in an electronic age.

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

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn't even imagined just a few years before.

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

Today, the great revolution in communication technology continues. From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a remarkable reservoir of information -- from Shakespeare's first sonnet to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values -- and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information -- from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has worked to build a framework for trust and security in this new world of electronic networks. We've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And to combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. This February, in his Cyber Security Summit, the President emphasized the primary role and responsibility of the private sector in ensuring computer and network security. As you know, most computers and networks that we rely upon every day are owned and operated by the private sector. It's only right that they -- not the government -- take the leading role in making security a standard part of the Internet.

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

Today we are taking a significant new step to update our export controls. Under new government regulations, we're taking down the barriers that prevent corporations from exporting encryption to governments and businesses in the European Union and eight other trading partners. We're also speeding up the time-to-market, by eliminating the thirty-day waiting period for exporting encryption goods.

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 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 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.

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.

[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, 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 11:35am

Gottheimer/ Swire

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

This week millions of Americans are waiting in line to buy a hotly anticipated book. No it's not Harry Potter. *[hold up book]* It's actually *Protecting Electronic Messaging* by John Podesta -- a book I wrote when I was on the Hill a few years ago. I'll be signing copies after the speech. Buy one for each of your children.

Today I want to return to some of the topics from my not-quite best-selling book -- particularly the issue of how to protect privacy and civil liberties, while also protecting public safety in an electronic age.

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

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn't even imagined just a few years before.

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

Today, the great revolution in communication technology continues. From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a remarkable reservoir of information -- from Shakespeare's first sonnet to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values -- and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information -- from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has worked to build a framework for trust and security in this new world of electronic networks. We've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And to combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. This February, in his Cyber Security Summit, the President emphasized the primary role and responsibility of the private sector in ensuring computer and network security. As you know, most computers and networks that we rely upon every day are owned and operated by the private sector. It's only right that they -- not the government -- take the leading role in making security a standard part of the Internet.

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

Today we are taking a significant new step to update our export controls. Under new government regulations, we're taking down the barriers that prevent corporations from exporting encryption to governments and businesses in the European Union and eight other trading partners. We're also speeding up the time-to-market, by eliminating the thirty-day waiting period for exporting encryption goods.

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 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 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.

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.

[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, 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 11:35am
Gottheimer/ Swire

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

This week millions of Americans are waiting in line to buy a hotly anticipated book. No it's not Harry Potter. *[hold up book]* It's actually *Protecting Electronic Messaging* by John Podesta -- a book I wrote when I was on the Hill a few years ago. I'll be signing copies after the speech. Buy one for each of your children.

Today I want to return to some of the topics from my not-quite best-selling book -- particularly the issue of how to protect privacy and civil liberties, while also protecting public safety in an electronic age.

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

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn't even imagined just a few years before.

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

Today, the great revolution in communication technology continues. From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a remarkable reservoir of information -- from Shakespeare's first sonnet to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values -- and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information -- from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has worked to build a framework for trust and security in this new world of electronic networks. We've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And to combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. This February, in his Cyber Security Summit, the President emphasized the primary role and responsibility of the private sector in ensuring computer and network security. As you know, most computers and networks that we rely upon every day are owned and operated by the private sector. It's only right that they -- not the government -- take the leading role in making security a standard part of the Internet.

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

Today we are taking a significant new step to update our export controls. Under new government regulations, we're taking down the barriers that prevent corporations from exporting encryption to governments and businesses in the European Union and eight other trading partners. We're also speeding up the time-to-market, by eliminating the thirty-day waiting period for exporting encryption goods.

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 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 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.

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.

[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, 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 11:35am

Gottheimer/ Swire

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

This week millions of Americans are waiting in line to buy a hotly anticipated book. No it's not Harry Potter. *[hold up book]* It's actually *Protecting Electronic Messaging* by John Podesta -- a book I wrote when I was on the Hill a few years ago. I'll be signing copies after the speech. Buy one for each of your children.

Today I want to return to some of the topics from my not-quite best-selling book -- particularly the issue of how to protect privacy and civil liberties, while also protecting public safety in an electronic age.

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

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn't even imagined just a few years before.

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

Today, the great revolution in communication technology continues. From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a remarkable reservoir of information -- from Shakespeare's first sonnet to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values -- and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information -- from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has worked to build a framework for trust and security in this new world of electronic networks. We've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And to combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. This February, in his Cyber Security Summit, the President emphasized the primary role and responsibility of the private sector in ensuring computer and network security. As you know, most computers and networks that we rely upon every day are owned and operated by the private sector. It's only right that they -- not the government -- take the leading role in making security a standard part of the Internet.

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

Today we are taking a significant new step to update our export controls. Under new government regulations, we're taking down the barriers that prevent corporations from exporting encryption to governments and businesses in the European Union and eight other trading partners. We're also speeding up the time-to-market, by eliminating the thirty-day waiting period for exporting encryption goods.

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 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 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.

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.

[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, 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.

● Michele Ballantyne

04/27/2000 06:42:26 PM

Record Type: Record

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

cc:

Subject: YPO Speech Information

if we do new econ/accomplishments for this, will it still be so difficult? he's the first speaker.

----- Forwarded by Michele Ballantyne/WHO/EOP on 04/27/2000 06:31 PM -----



Fern Mechlowitz

04/24/2000 05:52:50 PM

Record Type: Record

To: Joshua S. Gottheimer/WHO/EOP@EOP, Michele Ballantyne/WHO/EOP@EOP

cc: Scott Hynes/WHO/EOP@EOP, Rachael F. Goldfarb/OPD/EOP@EOP

Subject: YPO Speech Information

There will be 130 CEO's at this briefing (many of them are bringing their spouses, which may put the audience at 200 or so). Jay has told us that they are CEO's of mid-sized companies-- the main reason why we do this briefing every year is because the President is friends with the YPO President. (YPO is basically a networking business group that offers activities/meetings for CEOs to get to know one another and make contacts.) They are in DC for a few days, meeting with many government leaders.

Anyway- It is 1.5 hour briefing. John is set to speak first at 10am. John can speak about anything that he would like--- He can talk about our agenda for the coming year, or any hot issue of the week.

The Program is as follows:

10am-- Mary Beth Cahill introduces John. He speaks for 10 minutes, followed by Q&A.

10:30am- Barshefsky speaks and takes Q&A. She is taking about China/PNTR.

11:00am- The President may drop-by (it is listed as optional on his schedule).

The President's May 1997 Speech to this group can be found at: (I also have it in hard copy.)

<http://www.pub.whitehouse.gov/uri-res/l2R?urn:pdi://oma.eop.gov.us/1997/5/19/7.text.1>

Let me know what you want me to do for this... If John wants to use a general accomps/agenda speech, I can certainly pull a draft together for you, Josh. Let me know. thanks, Fern

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

Draft 07/12/00 11:35am
Gottheimer/ Swire

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

This week millions of Americans are waiting in line to buy a hotly anticipated book. No it's not Harry Potter. *[hold up book]* It's actually *Protecting Electronic Messaging* by John Podesta -- a book I wrote when I was on the Hill a few years ago. I'll be signing copies after the speech. Buy one for each of your children.

Today I want to return to some of the topics from my not-quite best-selling book -- particularly the issue of how to protect privacy and civil liberties, while also protecting public safety in an electronic age.

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

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn't even imagined just a few years before.

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

Today, the great revolution in communication technology continues. From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a remarkable reservoir of information -- from Shakespeare's first sonnet to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values -- and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information -- from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has worked to build a framework for trust and security in this new world of electronic networks. We've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And to combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. This February, in his Cyber Security Summit, the President emphasized the primary role and responsibility of the private sector in ensuring computer and network security. As you know, most computers and networks that we rely upon every day are owned and operated by the private sector. It's only right that they -- not the government -- take the leading role in making security a standard part of the Internet.

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

Today we are taking a significant new step to update our export controls. Under new government regulations, we're taking down the barriers that prevent corporations from exporting encryption to governments and businesses in the European Union and eight other trading partners. We're also speeding up the time-to-market, by eliminating the thirty-day waiting period for exporting encryption goods.

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 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 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.

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.

[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, 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 11:35am
Gottheimer/ Swire

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

This week millions of Americans are waiting in line to buy a hotly anticipated book. No it's not Harry Potter. *[hold up book]* It's actually *Protecting Electronic Messaging* by John Podesta -- a book I wrote when I was on the Hill a few years ago. I'll be signing copies after the speech. Buy one for each of your children.

Today I want to return to some of the topics from my not-quite best-selling book -- particularly the issue of how to protect privacy and civil liberties, while also protecting public safety in an electronic age.

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

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn't even imagined just a few years before.

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

Today, the great revolution in communication technology continues. From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a remarkable reservoir of information -- from Shakespeare's first sonnet to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values -- and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information -- from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has worked to build a framework for trust and security in this new world of electronic networks. We've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And to combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. This February, in his Cyber Security Summit, the President emphasized the primary role and responsibility of the private sector in ensuring computer and network security. As you know, most computers and networks that we rely upon every day are owned and operated by the private sector. It's only right that they -- not the government -- take the leading role in making security a standard part of the Internet.

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

Today we are taking a significant new step to update our export controls. Under new government regulations, we're taking down the barriers that prevent corporations from exporting encryption to governments and businesses in the European Union and eight other trading partners. We're also speeding up the time-to-market, by eliminating the thirty-day waiting period for exporting encryption goods.

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 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 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.

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.

[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, 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 11:35am
Gottheimer/ Swire

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

This week millions of Americans are waiting in line to buy a hotly anticipated book. No it's not Harry Potter. *[hold up book]* It's actually *Protecting Electronic Messaging* by John Podesta -- a book I wrote when I was on the Hill a few years ago. I'll be signing copies after the speech. Buy one for each of your children.

Today I want to return to some of the topics from my not-quite best-selling book -- particularly the issue of how to protect privacy and civil liberties, while also protecting public safety in an electronic age.

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

More than a hundred and fifty years ago, not too far from where we sit today, Samuel Morse sent the first telegraph message. With the touch of a finger, he shattered barriers of time and space, opening up a world of possibility that wasn't even imagined just a few years before.

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

Today, the great revolution in communication technology continues. From small towns to big cities, the Internet is bringing millions of people closer together, giving them new ways to find information and to stay in touch. When it was invented thirty years ago, there were just two computers exchanging very simple messages. Now there are almost 50 million households online, all with the same access to a remarkable reservoir of information -- from Shakespeare's first sonnet to the photos just taken of Mars.

The Internet, like Morse's telegraph, brings with it new found hope and opportunity. But it also brings new challenges to our most fundamental values -- and the need for new laws and new protections to maintain them. Because we are so interconnected, more people now have easier access to our most personal information -- from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber-property by defacing homepages and maliciously manipulating private information.

Over the last seven and a half years, our Administration has worked to build a framework for trust and security in this new world of electronic networks. We've taken action to ensure that what should be private, stays private, including the medical and financial records of our citizens. And to combat cyber-terrorism, we've introduced new legislation, increased law enforcement efforts, and coordinated public-private partnerships to build security and trust in online activities. This February, in his Cyber Security Summit, the President emphasized the primary role and responsibility of the private sector in ensuring computer and network security. As you know, most computers and networks that we rely upon every day are owned and operated by the private sector. It's only right that they -- not the government -- take the leading role in making security a standard part of the Internet.

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

Today we are taking a significant new step to update our export controls. Under new government regulations, we're taking down the barriers that prevent corporations from exporting encryption to governments and businesses in the European Union and eight other trading partners. We're also speeding up the time-to-market, by eliminating the thirty-day waiting period for exporting encryption goods.

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 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 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.

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.

[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, 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.

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

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

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

Don't know if all this background is necessary

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

raising

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

we are placing some of our most personal info on-line

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

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

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

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

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

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

Title III remained relatively untouched until the mid-1980s, when cellular telephone service, e-mail, and other computer-to-computer communication put new demands on outdated provisions of the 1968 privacy law. Like the phone in the 1920s, the new electronic technology of the 1980s raised new questions, which required new solutions. Most notably, Title III of the 1968 law only applied to wire and voice communications – not to wireless phone conversations

or e-mail. By that year, there were more than 7,000 Americans using cell phones, and more than 400,000 using electronic mail. In fact, by 1984, the Internet itself had grown to 1,000 users.

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

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

But ECPA -- like its predecessors -- has, in many ways, become outdated by new advances in computer technology and electronic communication. Our country, and the world, is increasingly more digital -- increasingly more interactive. Since the passage of ECPA, we've seen the mass development and use of the World Wide Web.

Today there are more 360 million cell phone users, and more than 50 million households on-line in the United States -- an increase of over 1250% since 1984 alone. And more than ~~over~~ 1.4 billion e-mails change hands each and every day. ^{As they did in the past} Moreover, computer users today don't just send message through their external modems, nor do they store information on their computers the way they did in the 1980's. Now many of them send e-mail through web sites like Yahoo, or through Internet service providers, like AOL; and they download files and e-mails on to servers at work and at home. ~~X~~ And a growing number of Americans -- 2.2 million -- log on to their e-mail through cable modems, a means of connection that wasn't even considered in ECPA. In fact, until the late 1980s, no one even thought that the cable going into your home ^{cable} ~~would~~ be used for anything but television programs. To protect the privacy of home viewers, the cable laws passed in 1986 made tapping a cable line even more difficult than tapping a phone call.

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

What does this mean? It means that data stored on networks is not afforded full privacy protection. That many of the protections in the wiretap law do not apply to email and other Internet protections. That ISP customers are not entitled to ~~note~~ ^{know} when personal information is

subpoenaed in civil lawsuits. And that ^{finally, their are} inconsistent standards ^{that} apply to government access to information ~~depending on the type of technology used.~~ \ oK

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

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

Second, we need to achieve *harmonization* of how the laws apply to different forms of communication. As I mentioned, the current law sets stricter standards for law enforcement access to "wire" communications such as telephone calls than ~~for~~ ^{to} "electronic" communications such as e-mail. In our era of rapid technological change, one of the Administration's central principles has been *technology neutrality* -- the idea that the government and the laws should be generally neutral between different technologies. 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, when e-mail and other "electronic" communications are relied upon ~~similarly to phone calls,~~ we believe that the same legal protections should apply. These protections include high-level approval within the Department of Justice, use ^d only for the most serious crimes, and suppression of evidence in court if the rules are not followed.

At the same time, we propose to change the standards that apply to cable services. Under the current Cable Act, even where there is clear proof of serious crimes, law enforcement officials cannot gain access to subscriber records ~~unless~~ ^{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-mail ~~and~~ 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 ^{the} law enforcement authorities ability ^{of} to address unlawful conduct, but also to enhance privacy and civil liberties on the Internet ^{at the same time}.

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} bewildering variety of companies that offer local, long distance, and wireless services. ^{Because of this,} Tracing a phone call often require separate subpoenas in the various courts where each of the companies operates. The problem in tracing Internet communications to their source can be even worse. The structure of the Internet means that communications are routinely shuttled among many nodes, often in different federal court districts.

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

In the early years of our republic, Thomas Jefferson said, "America's institutions must move forward hand-in-hand with the progress of the human mind." Today, the ^{scope} progress of the human mind ^{is certainly} ~~is certainly~~ ^{understanding} ~~is certainly~~ ^{expanding} racing forward at ^{exponentially} ~~break-neck speed~~ ^{speed}. Technology is opening up a new world of possibility -- but it is also challenging our privacy in ways we might never have imagined. In the right hands, the computer has become an indispensable tool for education, business, research and development. But in criminal hands, the same computer becomes a tool of destruction. As in any era of great progress, we must work together to ensure that our ^{system of} ~~just the law~~ democracy and our laws keep pace -- and that we protect our civil liberties, ^{most importantly} ~~not just the law~~ enforcement mechanisms that were instituted to preserve them.

by modernizing the

Q: How does the Administration's proposal compare to other legislation now before the Senate Judiciary Committee?

A: The Administration proposal addresses many of the same issues considered in the principal bills before the Senate Judiciary Committee, and offers an appropriate balancing of the existing proposals. The Administration bill contains important privacy-enhancing provisions that are in the Leahy bill (S. 2430) but not currently in the Hatch-Schumer (S. 2448) and Kyl-Schumer (S. 2092) bills. The Administration proposal does contain a number of important provisions contained in S. 2448 and S. 2092 that will make law enforcement more effective in addressing cyber-crime.

The Administration bill and the Hatch-Schumer bill (S. 2448) have significantly similar provisions for: one stop for a trap-and-trace order; restricting mandatory sentences for computer fraud to only serious felonies; treatment of juvenile offenders; and civil and criminal forfeiture provisions. The bills also address the Cable Act issue, but in different ways. The Administration bill would treat violations of the Computer Fraud and Abuse Act under \$5,000 as a misdemeanor, rather than as a felony under Hatch-Schumer.

The Administration bill and the Kyl-Schumer bill (S. 2092) have significantly similar provisions for: one-stop for a trap-and-trace order; emergency exception to trap and trace for ongoing, felony-level computer attacks; restricting mandatory sentences for computer fraud to only serious felonies; treatment of juvenile offenders; and civil and criminal forfeiture.

The Administration bill and the Leahy bill (S. 2430) both would elevate the protections for intercepting "electronic" communications up to the same level as for "wire" communications such as phone calls. The Leahy bill and the Administration bill would allow aggregation of small computer attacks to meet the \$5,000 threshold for felony violations of the Computer Fraud and Abuse Act. The bills would both address how to update the definitions of "pen register" and "trap and trace devices", in somewhat different ways.

All of the bills would apply to attacks on computers located outside of the United States.

ASSURING SECURITY AND TRUST IN CYBERSPACE

White House Chief of Staff John Podesta today, in a speech at the National Press Club, announced important measures to assure the security and trust of Americans in cyberspace. His speech emphasized the themes of *updating* law enforcement authorities for the Internet age, *harmonizing* the rules that apply to different technologies such as telephones and e-mail, and *balancing* important values. He proposed legislation that would give law enforcement important new tools to pursue criminals through cyberspace while also boosting citizens' fundamental rights to privacy in the electronic age. Mr. Podesta also announced new rules that will update encryption export controls.

A FRAMEWORK FOR SECURITY AND TRUST IN CYBERSPACE

* *Private sector leadership.* As emphasized at the White House Cyber Security Summit in February, the private sector, which owns and operates most of the computers that Americans rely upon, has the responsibility to lead in computer and network security.

* *Government as a model citizen.* The federal government will continue to make itself a model for information security and privacy practices.

* *Public-private partnership.* The federal government will continue to work in partnership with the private sector to build security and trust in online activities, as set forth in the National Plan for Information Systems Protection issued earlier this year.

* *Preserving fundamental values, even as technology changes.* These values include protecting public safety, privacy and civil liberties; improving the quality of life for all Americans, such as through the promotion of electronic commerce and elimination of the digital divide; and furthering the educational and free speech potential of the Internet.

UPDATING TELEPHONE-ERA LAWS FOR THE INTERNET AGE

In certain specific instances, laws written for the telephone era will need to be updated for the Internet age. Key provisions of the legislation:

* *Modernize outdated telephone-era language.* Current law uses outmoded terms such as "phone lines" and hardware "devices." The proposed legislation would apply to other forms of electronic communication and apply equally to hardware and software.

* *Harmonize the standards for intercepting electronic, wire, and cable communications.* Current law has widely varying rules for when law enforcement can intercept a communication, depending on whether an individual uses e-mail, a phone call, or a cable modem. The proposal would raise the legal standard for intercepting e-mails to the longstanding and strict rules that

apply to intercepting telephone calls. For the first time, court orders authorizing interceptions of e-mails could be applied for only after high-level approval and only for serious crimes. Violations of these rules would lead to suppression of evidence in court. At the same time, the rules that apply to the growing use of cable modems would also be harmonized to the telephone standard, while preserving the current, especially strict rules limiting government access to cable television viewing records.

** Create a balanced updating for "trap and trace" orders.* "Trap and trace" orders allow law enforcement to identify who is calling or using an electronic means to contact an individual. The proposal would allow law enforcement to respond more effectively to computer attacks by stating that only one such order is needed to trace a call or Internet session back to its source through multiple carriers. (Just as today, such an order could not be used to intercept the contents of communications protected by the wiretap statute.) Tracing would be permitted without prior approval by a court in an emergency, such as when a computer system is actually under attack. On the other hand, to assure that such orders are issued only when appropriate, federal and state judges for the first time would independently review the factual basis for issuing such orders.

** Strengthen the computer hacking law.* The Computer Fraud and Abuse Act should be strengthened to take account of the full range of damages caused by computer attacks. Multiple small attacks should also be treated as one large attack. To match the punishment to the crime, mandatory jail time should be eliminated for less serious attacks. Violations of the Act could result in civil or criminal forfeiture.

** Improve sanctions against illegal wiretapping.* The proposal would increase penalties for violations of wiretapping laws. Illegally intercepted communications could be used in court, but only to prove the guilt or innocence of a person accused of illegal wiretapping activity.

** Juvenile offenders.* For serious computer attacks, federal prosecutors should have jurisdiction over juvenile offenders. In such cases, offenders would still be treated as juveniles rather than as adults.

UPDATING ENCRYPTION EXPORT POLICY

Today, the Administration is updating its policy for encryption exports to the European Union and other key trading partners to assure continued competitiveness of U.S. industry in international markets.

**License exception.* Under the new policy, U.S. companies can export under license exception (i.e., without a license) any encryption product to any end user in the 15 nations of the European Union as well as Australia, Norway, Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. Previous distinctions between government and non-government end users are removed for these countries. Further U.S. exporters will be permitted to ship their products to these nations immediately after submitting a commodity classification request to the Department of Commerce, instead of waiting for a completed technical review or incurring a

30-day delay.

THE WHITE HOUSE
Office of the Press Secretary

For Immediate Release

July 17, 2000

STATEMENT BY THE PRESS SECRETARY

Administration Updates

Encryption Export Policy

Today, the Administration is updating its policy for encryption exports to the European Union and other key trading partners, thus assuring continued competitiveness of U.S. industry in international markets.

Under the new policy, U.S. companies can export under license exception (i.e., without a license) any encryption product to any end user in the 15 nations of the European Union as well as Australia, Norway, Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. Previous distinctions between government and non-government end users are removed for these countries. Further, U.S. exporters will be permitted to ship their products to these nations immediately after they have submitted a commodity classification request for their product to the Department of Commerce. Exporters no longer have to wait for a completed technical review or incur a 30-day delay to ship their encryption products to customers in these nations.

These updates track with recent regulations adopted by the European Union that ease encryption exports to the same countries. Consistent with the Administration's January 2000 commitment, U.S. companies can continue to compete effectively in these markets.

The steps announced today continue our policy to serve the full range of national interests: promote electronic commerce, support law enforcement and national security, protect privacy, and maintain U.S. industry leadership in security technologies.

#

Gray, Wendy E. (NSA)

From: Maertens, Thomas R. (NONPRO)
Sent: Monday, July 17, 2000 9:36 AM
To: Stockwell, David B. (PRESS); @RUDMAN
Cc: @NONPRO - Export Controls; @PRESS - Public Affairs; @NESASIA - NE/South Asia; @RUSSIA - Russia/Ukraine; Black, Steven K. (VP)
Subject: London Telegraph --Ru/Iraq -- MODIFIED [UNCLASSIFIED]

Here are modified points: STILL DON'T HAVE IC CLEARANCE

(If Asked only)

-- We have seen the London Telegraph piece

-- We have no evidence that Russia has engaged Iraq in a deal to sell AA missiles

--The Russians have been observing UN sanctions

(FYI: Rosvooruzheniye, the Russian arms export agency, does have an office in Baghdad, but it is inactive, except possibly, for servicing previous equipment sold.)

-----Original Message-----

From: Stockwell, David B. (PRESS)
Sent: Monday, July 17, 2000 8:48 AM
To: @RUDMAN
Cc: @NONPRO - Export Controls; @PRESS - Public Affairs; @NESASIA - NE/South Asia; @RUSSIA - Russia/Ukraine
Subject: FW: Podesta Speech [UNCLASSIFIED]
Importance: High

Guidance. More to follow on Russia-Iraq.

-----Original Message-----

From: Maertens, Thomas R. (NONPRO)
Sent: Monday, July 17, 2000 8:38 AM
To: Brzezinski, Mark F. (RUE); @NONPRO - Export Controls
Cc: @RUSSIA - Russia/Ukraine; @PRESS - Public Affairs; @NESASIA - NE/South Asia
Subject: RE: Podesta Speech [UNCLASSIFIED]
Importance: High

Following talkers cleared with State:

-- Iran's successful test of a Shahab-3 is an indication that despite the changes taking place in Iran, the Government of Iran is still pursuing a long-range ballistic missile capability that could eventually threaten U.S. friends and allies in the region.

-- The USG is actively engaging the governments of the DPRK, China and Russia in nonproliferation discussions with the goal of persuading them to curtail the transfer of sensitive missile technology to Iran.

[Van Diepen and Cagan clear]

Revised Final 07/17/00 9am
Gottheimer/ Swire

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

White House aides have been known to write kiss and tell books. I'm slightly embarrassed to say that the only book I've ever written was Protecting Electronic Messaging – not exactly up there with All Too Human.

But today I want to return to some of the topics from that 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, I need to give you a little bit of history. More than a hundred and fifty years ago, not too far from here, 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, this 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 possibilities. 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. That's why we have to make sure the Internet is used to 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 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 electronic messages and commerce.

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 any 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 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 non-defense agencies. Unfortunately, the Congress still 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 updating our existing communications privacy laws for the Internet age. At the heart of the issue is the Fourth Amendment, which protects, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”

In 1787, a person’s most important “papers and effects” -- like diaries and letters -- were almost undoubtedly in their home or place of business. These papers were protected by the requirement of a warrant before the state could enter and search. But over time, with advances in technology, people no longer relied solely on paper and pen to communicate with one another. By the turn of the 20th Century, people 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. 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.

By 1984, Title III simply did not protect the conversations of the 7,000 Americans who were using cellular phones, and the 400,000 who were logging onto electronic mail.

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

Today, 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 explosion of the cell phone and the development and use of the World Wide Web.

Today there are more 95 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 the stringent Title III protections to the capture of e-mail that you send to your friends or business partners.

It doesn't include other important protections for electronic communications – like the scope of the crimes covered ... the need for Justice Department approval, ... and a statutory suppression rule for government violations.

What does all 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 and inconsistent 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 these important privacy 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 the Administration is forwarding to the Hill today that would make this happen. Congress is already considering proposals in this area, and I believe together we can work to get them done this year.

First, current statutes set standards that only apply to wiretaps – traditional hardware “devices” – not to software programs that can conduct the same surveillance. Such telephone-era laws should be clearly updated to apply to the Internet era where hardware and software can be interchangeable.

Our proposed legislation does that: It would amend statutes using outmoded language and that are hardware-specific, so that they are technologically neutral. In other words, the legislation would apply equal standards to both hardware and software surveillance.

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.

Our proposed legislation would harmonize the legal standards that apply to law enforcement's access to e-mails, telephone calls, and cable services. For more than 30 years, federal law under Title III has set a tough, but workable 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.

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 cannot gain access to subscriber records, unless the customer can first 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 a better *balance* amongst the sometimes competing goals of – 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's ability to address unlawful conduct, but also to enhance privacy and civil liberties on the Internet.

For example, we need to update current law governs 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 state or 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 various telephone or Internet providers. 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 steps that will protect our public safety while preserving our civil liberties.

Fourth, and finally, in response to what we have learned about hacking attacks, we must update the Computer Fraud and Abuse Act. The Act should be strengthened to take account of the full range of damages caused by computer attacks. Small attacks -- with under \$5,000 damage -- should be treated as a misdemeanor and not as a felony as proposed by some in Congress. However, multiple small attacks should be treated as one large attack and punished accordingly. And we should match punishments to the crime, by eliminating mandatory jail time for less serious attacks.

Let me conclude by quoting Thomas Jefferson, who 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 racing forward at an extraordinary pace.

Technological discoveries are opening up new worlds of possibility -- but they are also challenging our privacy in ways we never imagined. As in any era of great progress, we must work to ensure that our democracy and our laws keep pace with our advances -- and that we protect our privacy and civil liberties, and not just the law enforcement mechanisms that we’ve instituted to preserve them.

Thank you.