S. HRG. 105–627

PRIVACY IN THE DIGITAL AGE: ENCRYPTION AND MANDATORY ACCESS

HEARING

BEFORE THE

SUBCOMMITTEE ON THE CONSTITUTION, FEDERALISM, AND PROPERTY RIGHTS

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

ON

EXAMINING THE USE OF ENCRYPTION AND MANDATORY ACCESS IN DIGITAL COMMUNICATIONS, FOCUSING ON PROPOSALS TO BALANCE PRIVACY RIGHTS WITH LAW ENFORCEMENT CONCERNS

MARCH 17, 1998

Serial No. J–105–87

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
50–474 WASHINGTON : 1998

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-057514-1

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

STROM THURMOND, South Carolina	PATRICK J. LEAHY, Vermont
CHARLES E. GRASSLEY, Iowa	EDWARD M. KENNEDY, Massachusetts
ARLEN SPECTER, Pennsylvania	JOSEPH R. BIDEN, JR., Delaware
FRED THOMPSON, Tennessee	HERBERT KOHL, Wisconsin
JON KYL, Arizona	DIANNE FEINSTEIN, California
MIKE DEWINE, Ohio	RUSSELL D. FEINGOLD, Wisconsin
JOHN ASHCROFT, Missouri	RICHARD J. DURBIN, Illinois
SPENCER ABRAHAM, Michigan	ROBERT G. TORRICELLI, New Jersey
JEFF SESSIONS, Alabama	

MANUS COONEY, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Minority Chief Counsel*

SUBCOMMITTEE ON THE CONSTITUTION, FEDERALISM, AND PROPERTY RIGHTS

JOHN ASHCROFT, Missouri, *Chairman*

ORRIN G. HATCH, Utah	RUSSELL D. FEINGOLD, Wisconsin
SPENCER ABRAHAM, Michigan	EDWARD M. KENNEDY, Massachusetts
STROM THURMOND, South Carolina	ROBERT G. TORRECELLI, New Jersey
FRED THOMPSON, Tennessee	

PAUL CLEMENT, *Chief Counsel*
MICHAEL O'LEARY, *Minority Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

CHRONOLOGICAL LIST OF WITNESSES

ALPHABETICAL LIST AND MATERIAL SUBMITTED

APPENDIX

Questions and Answers

Additional Submission for the Record

PRIVACY IN THE DIGITAL AGE: ENCRYPTION AND MANDATORY ACCESS

TUESDAY, MARCH 17, 1998

U.S. SENATE,
SUBCOMMITTEE ON THE CONSTITUTION, FEDERALISM,
AND PROPERTY RIGHTS,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m., in room SD–226, Dirksen Senate Office Building, Hon. John Ashcroft (chairman of the subcommittee) presiding.

Also present: Senator Feingold.

OPENING STATEMENT OF HON. JOHN ASHCROFT, A U.S. SENATOR FROM THE STATE OF MISSOURI

Senator ASHCROFT. Good morning, and welcome to our hearing on Privacy in the Digital Age: Encryption and Mandatory Access. We are holding this hearing to raise awareness about the important privacy interests that are at stake in the debate over encryption policy. Many have approached this debate as if it were just a technology issue or solely a law enforcement issue, but there are important civil rights at risk as well.

To date, we in the Senate have heard a great deal about the needs of law enforcement in the digital age and the risk that robust encryption poses to the traditional methods employed by law enforcement. We have been told that law enforcement needs mandatory access to every individual's electronic messages and material. We have even heard that we need a new fourth amendment for the digital age.

At the same time, we have heard almost nothing about privacy interests of law-abiding citizens. There has been an insistence that we turn over the keys to our individual privacy to the Federal Government, but there has been little or no talk about safeguards or privacy. Apparently, innocent citizens are expected to trust the bureaucracy not to abuse them, as the IRS has done by shakedown audits or the FBI by handing over hundreds of sensitive files to political operatives in the White House.

The purpose of this hearing is to balance the debate by adding the privacy interests of all U.S. citizens to the discussion. After all, the fourth amendment to the Constitution is about balance, the balance between the legitimate interests of law enforcement and the privacy interests of the citizenry. The fourth amendment neither prohibits nor permits all searches. It recognizes the legitimate

needs of law enforcement by authorizing reasonable searches and respects individual privacy by prohibiting unreasonable searches.

The Founding Fathers recognized the importance of this balance. In no way did they favor the notion that a key to every home, diary, bank account, medical record, business plan, or investment should be provided to the Federal Government for use without the individual's knowledge.

Some might suggest that the views of the Founding Fathers are irrelevant to the debate on encryption because they could not envision this type of technology. But it is dangerous to underestimate the Founding Fathers. Thomas Jefferson invented the wheel cypher in the 1790's. This invention consisted of a spindle of 36 wooden disks with letters carved on the outside. This simple devise would provide robust encryption similar to that provided by the high-tech software that the FBI is so concerned about. Nonetheless, neither Thomas Jefferson nor any of the other Framers suggested that encryption should be banned or that the fourth amendment should be repealed. Instead, they opted for the balanced approach reflected in the Constitution.

Such a balance is missing from the policies embraced by the administration and from the Senate Commerce Committee's bill. Moving forward with such proposals would be an act of folly, causing severe damage to our constitutional guarantees. The FBI has argued that a system of mandatory access would make it easier for law enforcement to do its job. Of course it would, but it would also make things easier on law enforcement if we simply repealed the fourth amendment.

None of this is to say that law enforcement does not have legitimate and important concerns. It does. We must work to provide law enforcement with the necessary amount of access, but we must do so in a manner consistent with our constitutional freedoms.

The issue of encryption policy also has broad implications for the future of electronic commerce and the extent to which the United States maintains a global electronic trade surplus. This is not merely an issue for the technology sector, but instead is critical to the future of digital commerce. Privacy is critical not just for personal information, but for financial and business information as well.

Business Week has recently reported that 61 percent of adults responded that they would be more likely to go online if the privacy of their information and communications were protected. Simply put, strong encryption means a strong economy. Mandatory access, by contrast, means weaker encryption and a less secure, and therefore less valuable network.

Without the protection of privacy, the Internet is doomed to the status of an international party line or an international broadcast device that will never become a useful means of education, commerce, communication, or entertainment. This morning's hearing will give us an important opportunity to explore these issues and balance the debate.

After my colleague from Wisconsin has had an opportunity to give an opening statement, we will hear from Congressman Goodlatte, who has championed the encryption issue in the House. Next, Bob Litt of the Justice Department will provide the administra-

tion's perspective on these issues. Then we will hear from two panels of outside witnesses, including constitutional scholars and technology experts who will share their perspectives on the importance of privacy in the digital age.

Fundamentally, this debate and this hearing is about the relationship of U.S. citizens to our Government. We must take steps to balance their privacy rights and the legitimate concerns of law enforcement. There is no greater challenge for concerned citizens inside and outside Government than to ensure that our great constitutional traditions are enhanced, not compromised, in the face of new technology. I hope that this morning's hearing can serve as a modest first step in meeting that challenge.

I am pleased to call upon Senator Feingold from Wisconsin.

STATEMENT OF HON. RUSSELL D. FEINGOLD, A U.S. SENATOR FROM THE STATE OF WISCONSIN

Senator FEINGOLD. Thank you, Mr. Chairman, for calling this hearing on this very interesting and informative topic.

The importance of effective and trustworthy encryption cannot be exaggerated. The use of encryption is likely to reach into virtually every aspect of our lives. Indeed, encryption systems provide security to conventional and cellular telephone conversations, fax transmissions, local and widearea networks, personal computers, remote key entry systems, and radio frequency communication systems.

Perhaps the most obvious application of encryption is its use to protect Internet and electronic commerce. Reportedly, the Internet and other like data networks will become the ideal way to conduct business in the near future. The Internet obviously provides a quick and efficient medium for the display of goods and services and for the transfer of sensitive information, such as credit card numbers and medical records and bank transactions.

In reality, however, the Internet will never become the mecca of commerce if people do not trust that their transactions and communications conducted on the Internet will remain confidential. Who would be willing to shop on the Internet if they thought there might be a thief lurking out there on the Net waiting to steal his or her Visa number?

Or consider even a more commonplace issue. Think of all the information you have stored in your computer at work or at home—your taxes, your banking information, maybe even your first novel. Or think of all the sensitive information you transmit via e-mail. Encryption may be the only way to keep this information safe. In short, if we are to ever realize the great commercial and communications potential of the Internet, we must have sophisticated and effective encryption.

Unfortunately, however, Mr. Chairman, there is also a downside to encryption. First, encryption can backfire. If the key to a system is lost, a user can be locked out of his or her own data and communications. Or perhaps more importantly, there are significant public safety issues that are raised by the use, sale and exportation of encryption.

As reported by the FBI:

Encryption has been used to conceal criminal activity and thwart law enforcement efforts to collect critical evidence needed to solve serious and often violent criminal activities.

The same technology that prevents a hacker from stealing your credit card number can prevent a law enforcement officer, even if she has properly obtained a court order, from decrypting illegal information. Indeed, the FBI reports that encryption has already been used in a number of high-profile cases, including the Aldrich Ames spy case, the Ramzi Yousef World Trade Center bombing, and a child pornography ring where pornographic images of children were transmitted using commercially available encryption technology.

Most encryption products in use today are nonrecoverable. That means that there is a far lesser chance of a hacker breaching the integrity of encrypted data, but it also means that law enforcement cannot always obtain timely access to the plain text of encrypted criminal-related and legally seized communication of information. According to the FBI, court-authorized electronic wiretaps and searchers are two of the most important law enforcement investigative techniques used to fight crime and prevent terrorism. Nonrecoverable encryption has the potential, therefore, to completely frustrate these essential law enforcement tools.

Law enforcement is calling for a technological solution to the problem of nonrecoverable encryption, whether that system be key recovery or some other solution that allows them access to information so that they can effectively prevent and investigate crime. The FBI, the National Sheriffs Association, the National District Attorneys Association, the International Association of Chiefs of Police, and the National Association of Attorneys General, all strongly advocate for an encryption policy that does not preclude them from continuing to lawfully obtain information regarding criminal activity.

Mr. Chairman, as you well pointed out, any solution that allows for law enforcement to obtain such information, however, can also compromise the integrity of an encryption system. If there is another key or a back door the FBI can use to conduct surveillance or a search, there is another key or back door that a hacker can use to steal someone's lawfully held personal information.

So we must return to my first point. If there is a flaw or a hole in the confidentiality of an encryption system, users will not trust the system and the development of electronic commerce and communications will be significantly retarded.

There is also, of course, as the chairman has pointed out, the fundamental right to privacy that will be at least somewhat sacrificed. If an encryption user is denied the right to purchase nonrecoverable encryption or if she is required to place the key to her system in escrow, that user is deprived of the right to keep her personal, lawful information completely confidential.

We as a society would be saying to this encryption user that although it is highly unlikely you will use encryption for any unlawful purpose, we are going to, ex ante, mandate that you forfeit a portion of your privacy. Moreover, there are novel and serious fourth and fifth amendment issues raised by a policy that would compel the use of recoverable encryption.

We have to ask ourselves, should the Government be able to require that a person, prior to any evidence that this particular individual has or will commit a criminal act, be forced to supply the Government with quick and easy access to her personal information on the off chance that this person commits an unlawful act in the future, and would such a policy with regard to encryption be a violation of the fifth amendment?

Or even more fundamentally, should an encryption user be mandated to trust the Government to use the recovery system properly? How can the encryption user be sure that the key to her encryption system will not be abused or fall into the wrong hands? As noted by Thomas Jefferson in a statement to James Madison, any society that would trade a little liberty to gain a little safety will deserve neither and lose both.

So, in conclusion, Mr. Chairman, I believe it is quite obvious to all of us that we have a difficult task before us. In the end, we must reach a solution to this issue that balances the equally significant, important interests of law enforcement and personal privacy. I do not, however, think that these interests have to be mutually exclusive. Indeed, as I understand it, progress is being made between the various parties toward a solution that may be acceptable to all. If everyone participates in a good-faith discussion of this issue, I believe we can reach a solution together. And I think this hearing is a very good step in that direction, so I thank the Chair.

Senator ASHCROFT. Thank you very much.

It is my pleasure now to introduce Congressman Bob Goodlatte, who represents the Sixth District of the State of Virginia. He has taken the lead role in the House on a number of technology issues and has championed the Security and Freedom Through Encryption, what is called the SAFE Act, H.R. 695.

Thank you very much for coming to share your views with the committee, Representative Goodlatte, and if you would proceed.

STATEMENT OF HON. BOB GOODLATTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

Representative GOODLATTE. Mr. Chairman, thank you very much for holding today's hearing and for your leadership on this issue, and thank you for affording me the opportunity to participate. I very much appreciate both of you mentioning in your opening remarks Thomas Jefferson, of my State of Virginia, and his actions and words regarding the issues of privacy and freedom which are very much at stake in this issue.

I do have a prepared statement which I would ask that the committee accept for the record and I will speak extemporaneously about this issue.

Senator ASHCROFT. It will be received. Thank you very much.

Representative GOODLATTE. The legislation that you referred to which I have introduced in the House of Representatives has experienced a tremendous surge in the last 2 years as a result of the increasing awareness of the public, the business community, and privacy organizations regarding the lack of security in their electronic communications, whether it be cellular telephone communications or transactions occurring on the Internet.

When I first introduced this in the 104th Congress, we had about 45 cosponsors and a hearing was held late in that Congress on the issue. During this Congress, that support has grown to 250 Members of the House of Representatives, a substantial majority of the House. It has passed through now five House committees and is expected to go to the floor of the House sometime this spring.

The legislation has the support of a wide array of organizations, everybody from the American Civil Liberties Union to the National Rifle Association. There are not many bills introduced in Congress that both of those organizations support, but I am proud to have both of their organizations' support because of the concern across the political spectrum about protecting the right to privacy of American citizens.

It also has the support of the U.S. Chamber of Commerce, the National Association of Manufacturers, the Online Bankers Association, the Direct Marketing Association, the National Retail Federation, a whole host of business organizations not only in the software and hardware computer industry, but across the wide array of industries that do now and need to in the future utilize strong encryption to protect their business transactions and those of their customers and suppliers.

The legislation is vitally important because it does three things. It protects the privacy of American citizens by assuring that they will be able to use strong encryption in the future. It fights crime, and I think we should not minimize the importance of this at all. The FBI and others do have a legitimate concern about the misuse of encryption, but they should not pursue a policy that stunts or even prohibits the availability of strong encryption to the good guys, to law-abiding citizens. This is something that will assure people that their credit card on the Internet will be secure, their medical records will be secure, their industrial trade secrets will be secure.

But equally importantly, we should recognize that the lack of strong encryption today makes many of the institutions in this country vulnerable to those same criminal hackers or terrorists that the FBI is concerned about, and we could face a crisis of almost unprecedented proportions sometime in the near future if we do not change this Government's policy and promote access to strong encryption. The New York Stock Exchange, the Chicago Board of Trade, nuclear powerplants, the electric power grid of this country will all be vulnerable at some point in the future if we do not promote ever-increasingly strong use of encryption by the institutions that are so important to protect in this country.

The chairman of the House Subcommittee on Crime, Congressman Bill McCollum, of Florida, has cited studies finding that the theft of proprietary business information costs American industry from $24 billion to over $100 billion every year. The use of strong encryption can prevent a great deal of that crime because most of it occurs electronically.

Strong encryption also helps to fight terrorism. Without strong encryption, we will face a threat to this country in the near future, and as a result I think the best response to law enforcement raising these alarms about the misuse of encryption is to point out that while we have concerns about that and want to help them address

those concerns, the appropriate way to do that is not to limit access and create mistrust in encryption systems which I fear the proposals by the Director of the Federal Bureau of Investigation and others would create.

The Senator from Wisconsin's very fine remarks pointed out that there have been those who are already using encryption for misdeeds, and he cited several of those. It is important to point out that none of those criminals or terrorists filed their key with law enforcement or with a third party to make the recovery of that key possible to law enforcement. Nor would Muammar Qadhafi or Saddam Hussein or the Cali cartel do so in the future.

I think that this is the heart of the problem. What we will do is we will keep encryption out of the hands of law-abiding citizens. We will harm the industry that has achieved great success in our country. About 75 percent of all of the software sold in the world today is created in the United States. In the future, a great portion of this software will have strong encryption attached to it. Virtually any software used for data storage or data communication, which is, if you think about it, most uses of software, will have strong encryption attached to it. People will buy it in the United States or they will buy it overseas. If we don't change our export control laws as provided for in my legislation, they will be buying it overseas and we will greatly harm this industry.

The misuse of export control laws in the past has harmed other American industries, and I fear greatly that a misunderstanding of this issue and the continued perpetuation of the belief that encryption, which is not even a tangible item—it is not a bomb or a jet or a mainframe computer, but it is simply a mathematical algorithm, little 1's and 0's going through electronic wires—is not suitable for a massive export control program.

I would also point out that my legislation does not eliminate export controls, as the administration has on some occasions claimed. It allows the export of United States made encryption if those products are generally available in the marketplace, and the bill does not allow the export of sensitive military or weapons technology or the use of encryption attached to those technologies.

Relaxing the current export barriers will free U.S. industry to remain a leader in software, hardware, and Internet development. And by allowing our computer industry to market the highest technology with the strongest security features available, America will lead the way into the 21st century information age and beyond.

Hundreds of thousands, perhaps ultimately millions of American jobs are at stake in our failure to promote and protect this industry, and that is the third purpose of my legislation. The legislation does four things. It prohibits the administration from establishing a mandatory key escrow or key recovery system. It is certainly not at all harmful for businesses to want to have access to a key recovery system of their own choosing and utilize it in a manner that they choose.

But I have grave constitutional concerns about the Government's involvement, as the Senator from Wisconsin also noted, in telling people in advance who have committed no crime, who are simply law-abiding citizens—and we are talking here about virtually every citizen of the United States—that they, in advance, must take an

action to put the key to their computer in a location where law enforcement can access it without their knowledge.

This is analogous to the requirement if the Senate or the House or the Congress were to pass legislation requiring a U.S. citizen to take the key to their home or their safe deposit box to a third party or to the local police station and deposit it there, with the assurance that law enforcement will not use it unless they get a court order. But if they do get a court order, they are going to take that key, enter your home, enter your safe deposit box, without your knowledge, and copy or take anything that they deem to be appropriate.

This is a major erosion of our fourth amendment protections against search and seizure, for several reasons. First of all, this is very much different than a wiretap where an individual is simply listening in to an ongoing conversation. We are talking about a person's entire financial records, their entire medical records, their entire political involvement that they may choose to store in a computer being made accessible not only to law enforcement, but to any hacker or criminal or terrorist who chooses to target that third-party holder of the key or that Government holder of the key. And this will become the Achilles heel of our electronic communications system if we put these keys out there where they will be vulnerable to a wide array of other people.

And, again, I commend the Senator from Wisconsin for pointing out that this would be a major change in our constitutional law to affirmatively require individuals in advance of any wrongdoing on their part, even suspicion of wrongdoing on their part, to compromise their own security in this fashion.

And so I would urge the Senate to take action similar to the progress we have been making in the House and to reject those forms of this legislation that have been proposed by others that turn the legislation on its head and promote these domestic key recovery systems which we do not have in this country today and I pray we will never have in the future.

Mr. Chairman, I thank you for the opportunity to testify. I do have a couple of additional items that I would ask be made a part of the record. One is a study entitled "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption" prepared by a very distinguished group of cryptographers and computer scientists, including some of those who devised the public-private key encryption system that now allows us to have, when it is used properly, security on the Internet and in other forms of electronic communication; and, second, an article from the New York Times entitled "Support for Encryption Is Less Than U.S. Claims, Study Says." This article is about the efforts of our Government to convince other governments around the world that they should adopt a similar policy regarding the escrowing of these keys and points out, in my opinion, the overwhelming rejection of this by the European Union and other countries around the world, raising further the question of how this system could ever be workable because of the international nature of the Internet. Unless you had virtually 100-percent participation around this world, this system would not be workable, and we have very, very much less than that kind of support from our competitors and our allies around the world.

Senator ASHCROFT. The committee thanks you for those submissions and they will be received for inclusion in the record.

Representative GOODLATTE. Thank you, Mr. Chairman.

[The information referred to follows:]

[The study "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption" is retained in committee files.]

[From the New York Times, Feb. 9, 1998]

SUPPORT FOR ENCRYPTION IS LESS THAN U.S. CLAIMS, STUDY SAYS

(By Jeri Clausing)

WASHINGTON.—The Clinton administration is losing its battle to increase international controls over how reliably computer data can be scrambled to insure privacy, according to a report scheduled to be released Monday by an independent research group.

The administration has been lobbying members of the European Union and other industrialized nations to back its efforts to place controls on "strong encryption," a technology for scrambling data so effectively that the code cannot be broken and the content cannot be deciphered without a digital key.

Data encrypting is used increasingly to protect the privacy of financial transactions, medical records and business communications. The administration wants the ability to descramble all encrypted messages to keep tabs on criminals.

In a report scheduled to be released Monday, the Electronic Privacy Information Center, a Washington-based research group, says that its survey of 243 governments showed that the United States is virtually the only democratic, industrialized nation seeking domestic regulation of strong encryption.

That finding directly contradicts the Clinton administration's assertion in congressional hearings that it has the support of most nations on this issue.

David Sobel, who directed the study by the research group for the Global Internet Liberty Campaign, a civil-liberties advocacy group, said of the administration: "They make the claim that other countries are accepting the U.S. position on this, then in an attempt to make that a reality, our government launched a worldwide lobbying campaign on encryption policy."

William Reinsch, the undersecretary for export administration in the U.S. Commerce Department, denied that the study contradicted the administration's assertions.

"All the administration has ever said is that there are more countries that go farther than we do," he said. "The study confirms that. And what I've gone on to say is that in talks with other countries, they are moving in our direction. I don't think the atudy itself does anything to contradict that."

The report comes as Congress prepares to renew what has become a contentious debate on encryption policy. Currently, the United States controls only the export of strong encryption. But the administration is pushing for a system that would give a third party a set of spare keys to all scrambled data so that law enforcement agencies could gain easy access to otherwise uncrackable computer files. The Federal Bureau of Investigation is pushing for a mandatory key recovery system that would guarantee the agency "immediate" access to the communications and data of suspected criminals.

Key recovery, as such systems are known, is opposed by virtually everyone outside of law enforcement agencies, including groups as diverse as the American Civil Liberties Union and the National Rifle Association. Opponents argue that such systems would be analogous to being required to leave copies of your letters at the post office in case some day you were suspected of committing a crime.

The survey, based on direct questioning of officials in more than 200 nations and territories, found that in the "vast majority of countries, cryptography may be freely used, manufactured, and sold without restriction," according to the report.

"This is true for both leading industrial countries and for countries in emerging markets," the report says. "We also noted that recent trends in international law and policy suggest greater relaxation in controls on cryptography. There are a small number of countries where strong domestic controls on the use of cryptography are in place. These include Belarus, China, Israel, Pakistan, Russia, and Singapore. There are an even smaller number of countries that are currently considering the adoption of new controls. These include India, South Korea and the United States."

The report calls the policies of the United States "most surprising, given the fact that virtually all of the other democratic, industrial nations have few if any controls on the use of cryptography."

It goes on to observe that the administration's position "may be explained, in part, by the dominant role that state security agencies in the U.S. hold in the development of encryption policy."

France is a notable exception to the international trend, having one of the most restrictive encryption control policies in the world. But the movement there has been toward easing those controls, according to the report. Last August, Industry Minister Christian Pierret said that France would liberalize its encryption policies to "allow French companies to fully enter the market of electronic commerce currently dominated by U.S. companies."

Sobel said that the study was conducted, in part, "to test the administration's representations about the state of play around the world on these issues, because they have been pretty outspoken in congressional hearings in claiming that the U.S. policy is in line with what governments are inclined to do with respect to encryption issues."

Reinsch defended those claims. "What we are finding in talks with government after government is a recognition of the need to create key management infrastructure," he said.

Lynn McNulty, a retired associated director for computer security at the National Institute for Standards and Technology who now is director of government affairs for the RSA Data Security, a developer of commercial encryption software, said he was not surprised by the survey's findings.

"I don't see any clear consensus out there in the world," McNulty said. "I think the governments are equally divided on these issues and are not likely to try and follow the U.S. in trying to go down the path of the U.S. in the key recovery scheme."

Representative GOODLATTE. I would also like to thank the Center for Democracy and Technology for their efforts to adopt a legislative program which can be accessed on the Internet and gives a great deal of information to our citizenry about this issue and how they can communicate with all of us regarding their concerns.

Thank you.

Senator ASHCROFT. Thank you.

[The prepared statement of Representative Goodlatte follows:]

PREPARED STATEMENT OF REPRESENTATIVE BOB GOODLATTE

Mr. Chairman, I would like to thank the Subcommittee for holding today's important hearing on the issue of encryption and privacy protection in the Information Age. As you know, I have introduced legislation in the House—H.R. 695, the Security And Freedom through Encryption (SAFE) Act of 1997—to encourage the use of strong encryption by all Americans.

This much-needed, bipartisan legislation, which currently has 250 House cosponsors and is likely to come to the House floor this Spring, accomplishes several important goals. First, it aids law enforcement by preventing piracy and white-collar crime on the Internet. At a hearing during the last Congress on economic espionage, the Chairman of the House Subcommittee on Crime—Bill McCollum of Florida—cited studies finding that the theft of proprietary business information costs American industry from $24 billion to over $100 billion every year.

The use of strong encryption to protect proprietary business information would prevent this theft from occurring, which is one of the reasons why I have introduced the SAFE Act. If an ounce of prevention is worth a pound of cure, then an ounce of encryption is worth a pound of subpoenas.

Strong encryption also helps fight terrorism. Without strong encryption, our nuclear power plants, air traffic control networks, financial markets, and national security infrastructures are completely vulnerable against those who seek to do America harm.

Only by allowing the use of strong encryption can we hope to make digital communications, on-line transactions, and America's national infrastructures safe and secure. As the blue-ribbon National Research Council concluded, "If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can), it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical

information systema and networks against unauthorized penetration (which it can), it also supports the national security of the United States."

With the availability of strong encryption overseas and on the Internet, current export controls only serve to tie the hands of American business. According to a widely noted study in December 1995, failure to remove these export controls by the year 2000 will cost our economy $60 billion and 200,000 jobs. The current export controls are forcing America to surrender our dominance of the global marketplace.

The SAFE Act remedies this situation by allowing the export of generally available American-made encryption products. This is an important point which I would like to make very clear—the bill does not eliminate export controls, as the Administration has argued on many occasions. It allows the export of U.S.-made encryption if those products are generally available in the marketplace. The bill does not allow the export of sensitive military or weapons technologies.

Relaxing the current export barriers will free U.S. industry to remain the leader in software, hardware, and Internet development. And by allowing our computer industry to market the highest technology with the strongest security features available, America will lead the way into the 21st century information age and beyond.

This bipartisan legislation enjoys the support of members and organizations across the entire spectrum of ideological and political beliefs. The SAFE Act enjoys this support not only because it is a common-sense approach to solving a serious problem, but also because ordinary Americans' privacy and security is being assaulted by this Administration.

The Administration continues to enforce antiquated encryption policies that threaten the personal privacy of law-abiding Americans. The Administration's approach, commonly called "key recovery" encryption, would require computer users to affirmatively give the government access to their private information and communications without their knowledge.

In addition to the feasibility questions surrounding the Administration'a policy, its approach raises serious constitutional questions as well. First Amendment guarantees of freedom of speech, Fourth Amendment protections against unreasonable searches and seizures, and Fifth Amendment rights against self-incrimination are all implicated by the Administration's proposals. I should note as well that the Administration'a current export control scheme has already been ruled unconstitutional by one federal court.

The Administration is proposing an Industrial Age solution to an Information Age problem. The SAFE Act, on the other hand, prevents the Administration from placing roadblocks on the information superhighway by prohibiting the government from mandating a back door into the computer systems of private citizens and businesses. Additionally, the SAFE Act ensures that all Americans have the right to use any security system they choose to protect their confidential information, while applying criminal penalties to those who use encryption to hide evidence from law enforcement or cover up federal felonies.

With millions of communications and transactions occurring on the Internet every day, American citizens and businesses must have the confidence that their private information and communications are safe and secure. That is precisely what the SAFE Act will ensure.

Mr. Chairman, thank you for holding today's important hearing and for allowing me the opportunity to testify. I would be happy to answer any questions you or the other members of the Subcommittee may have.

Senator ASHCROFT. It is my pleasure now to introduce Bob Litt, who serves as Deputy Assistant Attorney General at the Department of Justice. He has agreed to join us today to present the administration's views on encryption, and we are very pleased to welcome you and to thank you for being willing to make this appearance.

Mr. Litt.

STATEMENT OF ROBERT S. LITT, PRINCIPAL ASSOCIATE DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. LITT. Thank you, Mr. Chairman. In the interest of completeness, I should let you know that my position is now Principal Associate Deputy Attorney General, which is one word longer, and my kids can't figure out what the difference is.

Senator ASHCROFT. Well, thank you, thank you. Principal Associate Deputy Attorney General?

Mr. LITT. That is correct.

Senator ASHCROFT. Great.

Mr. LITT. Mr. Chairman, members of the subcommittee, thank you for the opportunity to appear today and present the views of law enforcement on the important issue of encryption. And I want to emphasize that the administration's goals on encryption are shared not only by the Department of Justice, but also, as Senator Feingold mentioned before, by the National Association of Attorneys General, the National District Attorneys Association, the International Association of Chiefs of Police, and the National Sheriffs Association. There is a very strong law enforcement consensus on this issue.

I would like to begin by clarifying the Clinton administration's recent initiatives on encryption. Two weeks ago, we began an intensive dialog between industry and law enforcement. Our goal in this process is to bring the creative genius of America's technology leaders to bear in trying to create and develop technical, market-savvy solutions that will enable Americans to realize the benefits of strong encryption while continuing to protect public safety and the national security.

We are not wedded to any particular technical approach. We are confident that American industry can come up with creative solutions. I am pleased to report that in our initial discussions with leaders of a number of high-tech companies, we have found them willing to work cooperatively with us in recognizing the important national security and public safety interests that are at stake. We think that a constructive dialog is far better than a legislative donnybrook.

Let me say in passing, by the way, that I have a much more complete written statement that I would ask to be part of the record. I am just going to summarize that orally.

Senator ASHCROFT. We thank you for your willingness to summarize and we would gratefully receive for the record your written statement.

Mr. LITT. Thank you, Mr. Chairman.

I do want to be clear that law enforcement strongly supports the use of strong encryption. We want to do what we can to encourage it. As Representative Goodlatte and as you both pointed out, encryption has important benefits for law enforcement and for individual privacy. Indeed, the role of the Department of Justice includes protecting privacy and intellectual property through enforcement of a number of statutes that the Congress has passed, such as the Economic Espionage Act that was passed by the last Congress.

Strong encryption is also essential to ensuring the growth and development of electronic commerce. But unbreakable encryption also presents a clear danger to our safety as individuals and as a nation. If unbreakable encryption becomes widespread, law enforcement will lose the benefit of valuable tools that are essential to protect public safety and the national security.

Court-ordered wiretaps which the Congress has authorized would become unintelligible. Information stored on computers by crimi-

nals which we can seize today pursuant to a warrant would become unreadable. Financial transactions of money launderers would become untraceable. In short, our ability to investigate and prosecute criminals such as drug dealers, terrorists, child pornographers, con artists, and many others would be greatly compromised.

Mr. Chairman, these are not theoretical concerns. When I was a Federal prosecutor, I found that the little black book that a drug dealer kept was often invaluable evidence that we could use to convict him and his confederates. We were able to seize these by a variety of legal and fully constitutional means. Today, that little black book might be one of the new electronic pocket organizers. Tomorrow, that pocket organizer might be encrypted and we would be absolutely unable to use that information.

I cannot emphasize for you strongly enough that as encryption becomes more and more widely available, the public safety and the national security will be endangered unless we act responsibly. Some people have suggested that law enforcement can actually break any encryption, that we have magic super computers hidden away somewhere that can do this. As I am sure you know, that is not so.

It was widely reported that one group managed to break a message that had been encrypted with 56-bit DES. However, they needed 14,000 computers to do it and it took them 4 months to decrypt a single message using those 14,000 computers. Mr. Chairman, tell the Jefferson City Police when they are wiretapping a kidnapper to try to save somebody's little girl's life that all they have to do is round up 14,000 computers and get them to work for 4 months to decrypt each conversation that they are intercepting. I think that gives a sense of the magnitude of the problem that we are facing.

I think that this has been set up to a certain extent as a false dichotomy. Either we are going to have encryption or we are not going to have encryption, and the suggestion has been made that law enforcement doesn't want people to have encryption. Mr. Chairman, there is a way that we can both guarantee Americans the benefit of strong encryption and preserve law enforcement's ability to protect the public, and that is through encryption that provides a means for law enforcement to obtain the plain text of encrypted data under appropriate lawful authority.

This kind of technology will let Americans use strong encryption to protect their personal information and American business use strong encryption to protect their business secrets. But it will also let American law enforcement protect American citizens and businesses from terrorists and criminals. One way to do this would be through what is called key recovery, providing to a trusted third party a copy of the information needed to decrypt data. But I want to emphasize that we are not wedded to that particular solution to the problem.

Mr. Chairman, my written statement addresses at some length the constitutional issues that plain text recovery technology raises and I would like to very briefly summarize what the Department's views on these issues are. But, first, I would like to mention a couple of important caveats.

First, I want to emphasize that the administration is not seeking mandatory domestic controls on encryption. Our goal, as I said before, is to work voluntarily with industry. It is somewhat difficult to discuss in the abstract the constitutionality of mandatory plain text recovery systems, since they could take many possible forms and different constitutional results might follow from different regimes.

The second point I want to make is that the issues raised by encryption are novel ones. The spectacular growth of the digital world has created many confounding legal issues that the Congress, the courts, the administration, and our society at large are wrestling with. But with these caveats, it is our best judgment that a mandatory plain text recovery regime, if appropriately structured and with appropriate safeguards, could comport with constitutional doctrine.

We believe that a plain text recovery regime could comply with the fourth amendment as long as the standards for seeking evidence by warrants or otherwise were not lessened; that is to say, today we need probable cause to obtain a search warrant to obtain your business records. We should still need the same probable cause to obtain those records in the future if they are encrypted.

And let me say in this regard that we are not talking about a lessening of privacy under this regime. We are talking about an increase in privacy because people's records that today are freely available and unencrypted would be encrypted. The Government is still going to require the same kind of legal process to obtain those records.

We also believe that a plain text recovery regime could comply with the fifth amendment's prohibition against compulsory self-incrimination. For example, if manufacturers of encryption products were required to keep a copy of encryption keys for products they sold, there would be no testimonial compulsion exercised against the user of the encryption if the Government later obtained that key pursuant to lawful process. Even if the user is himself required to deposit a copy of the key with a third party, we believe that under the Supreme Court's cases this would not violate the fifth amendment, as I explained in more detail in my written statement.

Finally, we don't believe that mandatory plain text recovery would violate the first amendment. While the arguments here are somewhat complex and analogous questions are before the courts now in the *Karn* and *Bernstein* cases involving export controls, at bottom we do not believe that an encryption program itself is speech, and we do not believe that the sorts of restrictions on encryption that we are talking about would impermissibly limit anyone's ability to speak.

Mr. Chairman, the suggestion has been made that because plain text recovery schemes could be abused by people, therefore they are unconstitutional. But that same analysis could be applied to search warrants or wiretaps or any one of a number of other technologies.

I want to conclude by emphasizing that law enforcement does recognize that we need a balanced approach in this area. We know that we can't get everything that we would want in our wildest dreams. There will always be those who use unbreakable encryption products, and some criminals will go free as a result.

We recognize, however, that we have to accept these limitations because there are other interests involved as well and that we need to balance those interests. Our approach does that. As I said, it recognizes the importance of both law enforcement and individual privacy and protects both.

And I want to make one last point. The Framers of our Constitution did not provide for an absolute right of privacy. They recognized in the Constitution that there were circumstances in which it is appropriate for law enforcement to obtain information even when an individual wants that information to be kept private. We can go to a judge and get a search warrant or a wiretap order upon probable cause.

Decisions as to where that line should be drawn are political and legal decisions, not scientific or business ones. They should be made by Congress and the courts, not by programmers or marketers. Policy should regulate technology. Technology should not dictate policy. There is no question that, one way or another, the law is going to have to take account of the changes that are brought about by encryption.

Mr. Chairman, I appreciate this opportunity to express the views of law enforcement on this important issue and I would be pleased to answer at this time any questions that you have.

Senator ASHCROFT. Thank you, Mr. Litt. Is it illegal to use encryption now in the United States?

Mr. LITT. No, sir.

Senator ASHCROFT. So that any level of encryption is now legal for people to use in this country?

Mr. LITT. That is correct.

Senator ASHCROFT. And your view is that we need to restrict that?

Mr. LITT. No, sir. What we are saying is we want to work with industry cooperatively. We are not looking for any kind of mandatory controls or restrictions domestically at this time. Our hope is that through conversations with industry and discussions where we lay out the problems that we think need to be solved and we invite industry's attention and participation in solving those problems that we will get a technological solution to these problems.

Senator ASHCROFT. If a person is required by Government to hand over a key, would that be a seizure that would trigger the fourth amendment, in your view?

Mr. LITT. For the Government to obtain the key, yes, that would be a seizure that would implicate the fourth amendment, yes, sir.

Senator ASHCROFT. If the Government took a set of my files and copied them all and returned the originals, but promised not to make any use of the files unless and until agents demonstrated to a magistrate that they had probable cause to analyze the files and that the files were relevant, would the original seizure pose any fourth amendment concerns, in your view?

Mr. LITT. Yes, it would.

Senator ASHCROFT. In the handful of cases in which encryption is encountered, how many times has the case been broken using traditional investigative measures? Do you know?

Mr. LITT. I can't get you that information specifically, but I do know that there are cases that we have had, Mr. Chairman, where we have encountered unbreakable encryption.

Senator ASHCROFT. Is it your view that if the Government requires you to deposit the key with a third party instead of with the Government that it obviates or somehow deletes the triggering of the fourth amendment?

Mr. LITT. We think, Mr. Chairman, that if Congress were to pass a regime that required, that it could be structured so as to comply with the fourth amendment, yes.

Senator ASHCROFT. Could you explain how it is that if the Government requires you to give a key to some third party that it could avoid that problem?

Mr. LITT. Because we would still be required to meet the traditional standards of probable cause or whatever else was imposed in the particular situation for the Government in order to obtain any of the information that the person has. We would not be affecting the underlying constitutional standard that limits the Government's ability to get information or evidence from individuals.

Senator ASHCROFT. Is it your view that the fourth amendment only applies to protect a citizen from an unreasonable search by the Government?

Mr. LITT. Yes, sir.

Senator ASHCROFT. What does law enforcement do when it intercepts a telephone conversation on a wiretap, but both parties are speaking in a code that appears to be gibberish?

Mr. LITT. We try to decode it, and we encounter frequently in narcotics cases that people do speak in codes.

Senator ASHCROFT. Am I correct that if agents have obtained a warrant to search a home and they find a computer, you believe they should be allowed to have the key to all the stored data only upon a showing of relevance?

Mr. LITT. I am not sure I understand the question.

Senator ASHCROFT. Am I correct that if agents have obtained a warrant to search a home and they find a computer, you believe they should be allowed to have the key to all the stored data only upon a showing of relevance?

Mr. LITT. I believe that the ability to obtain the key should depend upon the ability to obtain the underlying data. If we have probable cause to seize particular data on that computer, we should be able to obtain the key to decrypt it.

Senator ASHCROFT. What is that showing going to look like, given that the proceeding will be ex parte and the Government will not know the content of the encrypted information?

Mr. LITT. Ordinarily, in a situation such as you suppose, we would have gone to a magistrate and we would have presented information to the magistrate that would establish probable cause that a crime had been committed. Let us say that this person was a pedophile and had been exchanging communications trying to lure 13-year-old children to meet with him for sexual purposes. We would have established probable cause through a variety of other evidence to believe, No. 1, that that crime had been committed and, No. 2, that evidence of that crime would be found on the computer.

We have to meet that standard before we can get a warrant for the computer.

Senator ASHCROFT. So you would require an additional showing of probable cause to the magistrate to enter the computer?

Mr. LITT. I don't know what you mean by "additional." We have to show probable cause to believe that there is evidence on that computer in order to obtain a warrant to search the computer. That is true today, yes, sir.

Senator ASHCROFT. Senator Feingold.

Senator FEINGOLD. Mr. Litt, there is—I think you already cleared this up, but some confusion between the White House and where the FBI stands on this issue. As I understand it, the FBI appears to be calling for a key recovery system for domestic encryption, but the Vice President recently sent a letter to Senator Daschle noting, "The administration is not wedded to any single technological solution. The administration believes that the best approach is to pursue a good-faith dialog over the coming months between industry and law enforcement which can produce cooperative solutions rather than seeking to legislate domestic controls."

Do I understand you to say that the administration position is different, then, from the FBI on this?

Mr. LITT. No. I think the administration's position, including law enforcement's position on this, is as set forth by the Vice President. I think that we are all looking at this point not to impose any mandatory legislation, but to work cooperatively with industry to find whatever solutions are available out there.

Senator FEINGOLD. And you are representing that that is the FBI's position as well?

Mr. LITT. Yes, sir.

Senator FEINGOLD. OK. With regard to some of the issues the chairman was raising, is it your position that law enforcement should have to attain the same court order or warrant to conduct a wiretap or to seize encrypted material as it would to gain access to any other type of information?

Mr. LITT. If I understand your question correctly, the answer is yes. In the wiretap context, we would have to meet the very high various evidentiary thresholds that apply before we can get a wiretap and we should be able to intercept the communication, whether it is encrypted or not, if we can meet those thresholds.

Senator FEINGOLD. And then do you support the amended McCain-Kerry bill that would also require law enforcement to obtain an additional court order declaring that the encrypted material is relevant?

Mr. LITT. I have not had an opportunity to review the amended Kerry-McCain bill. Obviously, we think that Congress has the power to impose limitations for the greater protection of privacy than would be required by the fourth or fifth amendments, and we would certainly be prepared to work with you to establish any such precautions that would, on the one hand, not impose undue burdens on law enforcement, but also would give people the kind of assurances that they need that these are, in fact, going to be adequately protected.

Senator FEINGOLD. I appreciate that answer. Can you tell me about any cases in which encryption has frustrated law enforcement's efforts to obtain unlawful information?

Mr. LITT. I do know—and I obviously can't go into a lot of detail here, but I do know that there have been hacker cases, one in particular that I am aware of, where a hooker who was breaking into Government computers stored encrypted data on his machine and as a result of that we were unable to ascertain all the data that he had downloaded or what he had done with it. There are also narcotics conspiracies where we are getting wiretap information and we are starting to occasionally see encryption in those that frustrates us from learning who the other conspirators are, when they are bringing drugs in, and so on.

Senator FEINGOLD. Thank you, Mr. LITT. Mr. Chairman, I have to go to the beginning of the markup on the Budget Committee for the budget, but I really do appreciate the opportunity to participate in the hearing to this point and I look forward to working with you on this issue, Mr. Chairman.

Senator ASHCROFT. Thank you, Senator Feingold.

I thank the witness for coming, and let me see if I can—I want to thank the Principal Associate Deputy Attorney General. [Laughter.]

Mr. LITT. Thank you, Mr. Chairman.

Senator ASHCROFT. I appreciate your remarks and your contribution to the committee. Thank you.

[The prepared statement of Mr. Litt follows:]

PREPARED STATEMENT OF ROBERT S. LITT

Thank you, Mr. Chairman and members of the Subcommittee, for this opportunity to discuss with you the important and complex issue of encryption. Encryption holds the promise of providing all of us with the ability to protect data and communications from unlawful and unauthorized access, disclosure, and alteration. Moreover, encryption can help prevent crime by protecting a wide range of data as we and our valued information become more and more connected to each other and to potential adversaries through the spread of information networks. As a result, the law enforcement community supports the development and widespread use of strong encryption products and services.

At the same time, however, the widespread use of unbreakable encryption presents a tremendous potential threat to public safety and national security. Criminals and terrorists have already begun using encryption to conceal their illegal activities and to defeat important law enforcement and national security objectives. In developing our Nation's encryption policy, we must carefully balance the many different interests that the policy will affect. In seeking that balance, it is essential to understand both the promise and the peril that this technology holds, and to identify responsible ways forward that advance all of the competing interests.

I want to begin, Mr. Chairman, by clarifying the Clinton Administration's recent initiatives regarding encryption. For some time, the Administration's position has been to encourage the design, manufacture, and use of encryption products and services that allow for the plaintext of encrypted data to be recovered. The Administration's approach has in fact found support in the marketplace, in part because businesses and individuals need a routinely available method to recover encrypted information. For example, a company might find that one of its employees lost his encryption key, thus accidentally depriving the business of critically important and time-sensitive data. Or a business may find that a disgruntled employee has encrypted confidential information and then absconded with the key. In this type of case, a data recovery system promotes important private sector interests. Indeed, as the Government implements encryption in our own information technology systems, it also has a business need for plaintext recovery to assure that data and information that we are statutorily required to maintain are in fact available at all times. For these reasons, as well as to protect public safety, the Administration has been affirmatively encouraging the development of data recovery products, recogniz-

ing that only their widespread, ubiquitous use will both provide greater protection for data and protect public safety.

In further support of this goal, two weeks ago we set in motion a process of pursuing an intensive dialogue between industry and law enforcement. Our goal in this process is to bring the creative genius of America's technology leaders to bear in developing technical, market-savvy solutions that will enable Americans to realize the benefits of strong encryption while continuing to protect public safety and national security. We do not harbor any illusions that there is no magic technology, a silver bullet that addresses all the needs of the marketplace. But we think constructive dialogue in a variety of areas and fora is far preferable to a stalemate that arises from a battle of wills and rhetoric; working together is better than fighting legislative battles.

The Administration is not advocating any single product, technology, or even technical approach. Rather, we are flexible—provided that the resulting solutions and arrangements preserve the Nation's ability to protect the public safety and defend our national security. These are public interests of the highest order, shared by the Congress and by all of our law-abiding citizens. Industry has the technical know-how to develop commercially viable mechanisms that maintain the government's ability to safeguard its citizens, while protecting our citizens from unwarranted intrusions from any source.

Now let me describe in a little more detail the important law enforcement and national security interests that are at stake in the encryption debate. First, I want to reiterate that the Department of Justice supports the use of strong encryption. Law enforcement's responsibilities and concerns include protecting privacy and promoting secure commerce over our nation's information infrastructure. For example, we prosecute those who violate the privacy of others by illegal eavesdropping, hacking, or stealing confidential information. In the National Information Infrastructure Protection Act of 1996, at the request of the Administration, Congress provided further protection to the confidentiality of stored data. And the Department of Justice helps promote the growth of electronic commerce by enforcing the laws, including those that protect intellectual property rights and that combat computer and communications fraud.

Moreover, the Department of Justice, like other government agencies, realizes that our own information technology systems will increasingly require the use of strong encryption to provide appropriate security for the valuable and sensitive information that we hold on behalf of the American people. The Department, both as an enforcer of the law and as a consumer of encryption technologies, thus has a keen interest in the success of American industry in this area.

However, I don't think that it can reasonably be disputed that the unchecked spread of non-recoverable encryption will also endanger the public safety and our national security. People think of encryption primarily in the context of transmitted communications such as phone calls, and its effects on wiretaps. Indeed, it is absolutely essential that law enforcement preserve the ability to obtain the plaintext of information from lawfully authorized wiretaps and to authenticate this information in court. Court-ordered wiretaps are an essential tool for law enforcement in investigating and prosecuting some of our most important matters involving narcotics dealing, terrorism and organized crime.

But I'd like to focus for a moment on a slightly different aspect here: data stored on computers. It's very common, for example, for drug dealers or terrorists, or any other criminals for that matter, to keep records of their activities in notebooks or other written form. When I was an Assistant United States Attorney, I prosecuted several cases in which we arrested drug dealers and seized their "little black books" pursuant to search warrants or other valid legal authority. These notebooks provided invaluable evidence against the defendant and helped us identify and prosecute other members of the drug ring.

Today, however, we might find that the defendant is using one of the increasingly popular electronic organizers or personal information manager software programs to keep his records instead of a notebook. Or we might find that a swindler running a telemarketing scam has his records on a computer instead of in file cabinets. The switch from written to digital records does not undermine law enforcement interests—as long as the defendant hasn't encrypted the data. But if strong encryption becomes a standard feature, law enforcement will lose its ability to obtain and use this evidence. In fact, commonly available encryption products are already so strong that we cannot break them.

The same problem exists with respect to other types of criminals also. Ramzi Yousef, the mastermind of the World Trade Center bombing, used a laptop computer. Pedophiles who exchange child pornography via computer are already actively using encryption. White collar criminals and economic spies often use comput-

ers to steal our businesses' valuable intellectual property. I can't emphasize too strongly the danger that unbreakable, non-recoverable encryption poses: as we move further into the digital age, as more and more data is stored electronically rather than on paper, as very strong encryption becomes built into more and more applications, and as it becomes easier and easier to use encryption as a matter of routine, our national security and public safety will be endangered—unless we act responsibly.

Some people have suggested that this is a mere resource problem for law enforcement. They believe that law enforcement agencies should simply focus their resources on cracking strong encryption codes, using high-speed computers to try every possible key when we need lawful access to the plaintext of data or communications that is evidence of a crime. But that idea is simply unworkable, because this kind of brute force decryption takes too long to be useful to protect the public safety. For example, decrypting one single message that had been encrypted with a 56-bit key took 14,000 Pentium-level computers over four months; obviously, these kinds of resources are not available to the FBI, let alone the Jefferson City Police Department. Moreover, it is far easier to extend key lengths than to increase computer power. Indeed, 128-bit encryption is already becoming commonplace. In this environment, no one has been able to explain how brute force decryption will permit law enforcement to fulfill its public safety responsibilities.

We believe that the most responsible solution is the development and widespread use of encryption systems that, through a variety of technologies, permit timely access to plaintext by law enforcement authorities acting under lawful authority. I will refer to these systems, collectively, as plaintext recovery systems, although they can encompass a variety of technical approaches. The concept of key recovery, where the key to encryption is held by a trusted third party, is one such approach, but it is by no means the only one that would meet law enforcement's goals.

Some have suggested that law enforcement's access to the plaintext of encrypted data and communications that is evidence of a crime would violate constitutional rights. Although I will discuss in a moment the constitutionality of a mandatory recovery regime, let me begin by reiterating that no such mandatory regime exists, nor does the Administration seek one. Rather, the Administration's efforts have been to encourage the voluntary use of data recovery products. In this context, there is no doubt that the government's efforts are constitutional.

It is certainly difficult to understand how a voluntary regime might violate the Fourth Amendment. As with any kind of stored and transmitted data, it is axiomatic that the government may obtain both encrypted text and decryption keys pursuant to lawful process, which may include a wiretap order, a search warrant issued upon probable cause, a subpoena, or the consent of the party possessing the particular item. Each of these comports with the Fourth Amendment, and voluntary data recovery products do not change this analysis. Additionally, if an individual's encryption key were stored with a third party, Congress requires by legislation that, to compel production of the key, law enforcement would have to meet a standard higher than that required by the Fourth Amendment, much as the Electronic Communications Privacy Act requires a court order to obtain transactional data. If Congress were to address this issue, we would be pleased to work with you to determine the appropriate standard and mechanisms for obtaining keys.

The Subcommittee has requested that I address the legal issues that might be associated with a mandatory plaintext recovery regime. Again, let me restate that the Administration does not advocate such an approach, and believes that a voluntary solution is preferable. Nonetheless, I am prepared to discuss hypothetical legislation prohibiting the manufacture, distribution and import of encryption products that do not contain plaintext recovery technologies, so that the capability to decrypt encrypted data and communications is available to law enforcement upon presentation of valid legal authority.

In considering the Department's views on these issues, I would urge you to keep several caveats in mind. First, the constitutional issues that such a regime would present are undoubtedly novel ones. Indeed, the spectacular growth of the digital world has created many confounding legal issues that the Congress, the courts, the Administration, and our society at large are wrestling with. If history is any guide, changes in technology can lead to changes in our understanding of applicable constitutional doctrine. Moreover, these issues are particularly difficult to address in the abstract, because mandatory plaintext recovery could take a variety of forms. Nonetheless, and with these caveats, it is the best judgment of the Department of Justice that a mandatory plaintext recovery regime, if appropriately structured, could comport with constitutional doctrine.

Let me turn first to the Fourth Amendment. It should be remembered at the outset that the Fourth Amendment does not provide an absolute right of privacy, but

protects reasonable expectations of privacy by prohibiting unreasonable searches and requiring that a warrant issue only upon a finding of probable cause by a neutral and detached magistrate. A well-designed plaintext recovery regime would ensure that users' reasonable expectations of privacy were preserved. Any legislation in this area, whether or not it imposed plaintext recovery requirements, should not lessen the showing the government must make to obtain access to plaintext. If a search warrant for data was required before, it should be required under any new regime. By requiring the government to meet current constitutional thresholds to obtain plaintext, such a regime would, in our view, comply with the Fourth Amendment. Moreover, Congress could require under such a regime that even if law enforcement obtains a search warrant for data or communications, it would need additional authority, such as a court order, to obtain the key or other information necessary to perform any decryption if the information is encrypted.

Some have also argued that mandatory plaintext recovery regime would violate the Fifth Amendment's prohibition against compulsory self-incrimination. However, the Fifth Amendment generally prohibits only disclosures that are compelled, testimonial, and incriminating. If a manufacturer of an encryption product were required to maintain information sufficient to allow law enforcement access to plaintext, we believe that there would be no violation of the Fifth Amendment because no disclosure at all would be compelled from the user of the encryption product. If, on the other hand, a mandatory plaintext recovery regime required the user of an encryption product to store his key (or other information needed for recovery) with a third party in advance of using the product, we do not believe that such an arguably compelled disclosure would be testimonial as that term has been interpreted by the Supreme Court. In *Doe* v. *United States,* 489 U.S. 201 (1988), the Court held that an order compelling a person to execute a form consenting to disclosure of foreign bank accounts did not violate the Fifth Amendment because the form was not testimonial. The compelled disclosure of decryption information to a third party would not seem to be any more testimonial. Moreover, we doubt whether such a disclosure would be incriminating, because unless and until the encryption product is used in the commission of a crime, the key would pose no threat of incrimination against the user.

Finally, it has been suggested that a statutory restriction on the manufacture, import, and distribution of certain types of encryption products would violate the First Amendment. Opponents of encryption restrictions sometimes argue that the First Amendment protects the right of persons to speak in "code"—i.e., to speak in ciphertext—and that a restriction on the distribution of products that make a particular coded communication possible would be analogous to placing a restriction on the use of a foreign language. This First Amendment argument rests on the faulty premise that the creation or dissemination of ciphertext itself is constitutionally protected. But, unlike a foreign language, the ciphertext that is created by strong encryption products cannot be understood by the viewer or listener. When it is heard, such as on a wiretap of a telephone, ciphertext simply takes the form of unintelligible static. In written form, ciphertext may be in the form of letters, numerals and symbols, but no human being can read or "understand" it: it does not contain characters or words or symbols that represent or correspond to any other characters, words or symbols. Accordingly, ciphertext is not like a foreign language, the use of which can convey unique meaning and nuance to the listener or reader. Thus, ciphertext itself—as opposed to the underlying plaintext—has none of the properties of protected "speech" that the Supreme Court has traditionally identified, and, accordingly, the dissemination of ciphertext should not be entitled to First Amendment protection.

A second form of First Amendment argument focuses not on the ciphertext, but on the underlying plaintext. Under this theory, a prohibition on the manufacture or distribution of nonrecoverable encryption products would inhibit an alleged constitutional right of persons to obscure their communications in any manner they see fit. Even if legislation would impose such a practical limitation on the manner in which speakers may obscure their underlying communications, it could be drafted so as to pass muster as a permissible time, place and manner restriction—particularly since any such restriction on the "tools" of speech would be unrelated to any communicative impact of the underlying plaintext and the controls would leave open ample and robust alternative channels or methods for obscuring the underlying plaintext.

A related argument is that a communications infrastructure in which recoverable encryption is the de facto standard will impermissibly chill a significant quantum of speech because individuals' knowledge of law enforcement's ability to overhear and decipher communications and data will unduly deter them from communicating. But under such a system, the government would have no greater access to the con-

tent of private parties' communications than it currently has, and it is well-settled that the government's exercise of its established statutory powers to intercept and seize communications does not create such a "chilling" effect on speech as to transgress the First Amendment, so long as that power is exercised consistent with the Fourth Amendment, and for valid reasons authorized by atatute, such as to discover evidence of criminal wrongdoing. See, e.g, *United States* v. *Ramsey*, 503 F.2d 524, 526 n.5 (7th Cir. 1974) (Stevens, J.) (rejecting argument that "the very existence of wiretapping authority has a chilling effect on free speech and, therefore, * * * violates the First Amendment"); *Accord United States* v. *Moody*, 977 F.2d 1424, 1432 (11th Cir. 1992).

A final type of First Amendment argument often heard is that a restriction on the manufacture and distribution of certain types of encryption products would impermissibly restrict the ability of cryptographers, and others, to disseminate the computer code that is used by computers to transform plaintext into ciphertext. But that argument is based on the mistaken premise that dissemination of the code embedded in encryption products itself is necessarily a form of expression protected by the First Amendment. Most auch code is in the form of "object code." Object code is simply an immense string of "0"s and "1"s, representing a bewildering concatenation of thousands or millions of high and low voltage electrical impulses. As such, machine-"readable" cryptographic object codes can reveal neither to possible "readers" neither the ideas they embody, nor the manner in which the ideas are expressed. And this is especially true where such object code is embedded in a product such as a semiconductor chip, so that even the "0"s and "1"s cannot be discerned. Therefore, a restriction on the dissemination of encryption products containing object code would not violate the First Amendment.

The question would be somewhat more complicated with respect to source code—i.e., the instructions to the computer that human beings write and revise. Some persons do disseminate source code for communicative purposes. Nevertheless, we believe that a restriction on the dissemination of certain encryption products could be constitutional even as applied to those relatively infrequent cases in which such products are in the form of software that is disseminated for communicative reasons, because such a restriction could satisfy the "intermediate" scrutiny that the First Amendment provides for incidental restrictions on communicative conduct. As we have argued in litigation in the export-control context, such intermediate scrutiny would be appropriate because the government's reason for regulation source-code software would not be based on any informational value that its dissemination might have. Instead, regulation would be premised on the fact that such software—like all of the "encryption products" that would be regulated—has physical, functional properties that can cause a computer to encrypt information and thereby place plaintext beyond the technical capabilities of law enforcement to recover.

Once again, I would like to emphasize that I have presented our constitutional analysis of a mandatory plaintext recovery system to respond to the Subcommittee's request for our views on the legal issues associated with such systems. As I noted above, this constitutional analysis would depend significantly on the nature of the particular system Congress mandated and the findings which supported it; our analysis is entirely generic. Moreover, I would emphasize again here that it is not the policy of the Administration to seek mandatory plaintext recovery legislation; it is the Department of Justice's hope and expectation that the dialogue with industry that I spoke of earlier will yield outcomes that make sense from both a business and a public policy perspective.

Those who argue against preserving lawful government access to encrypted communications often say that the government should bow to the inevitable and accept, even embrace, the spread of unbreakable encryption, rather than trying to fight it. For example, one of my colleagues recently met with a representative of a large computer company who is critical of the Administration's encryption policy. This industry representative said that he recognized that encryption poses a problem for law enforcement, but that we should recognize that other technologies, such as cars, also create problems for law enforcement, yet we have managed. He said, "We don't ban cars, do we? Then why are you trying to ban encryption?"

Of course, I hope it is clear by now that the Government is not trying to ban encryption. Law enforcement supports the responsible spread of strong encryption. Use of strong encryption will help deter crime and promote a safe national information infrastructure.

But the more fundamental point raised by the analogy to the rise of the automobile is that society "managed" the automobile, not by letting it develop completely unfettered and without regard to public safety concerns, but first by recognizing that cars could cause substantial damage to the public safety, and then by regulating the design, manufacture, and use of cars to protect the public safety. Cars must

be inspected for safety on a regular basis. Cars are subject to minimum gasoline mileage requirements and maximum pollutant emission requirements. Cars built today must include seat belts and air bags. Perhaps most closely analogous, the laws of every jurisdiction in the United States closely regulate every aspect of driving cars on the public streets and highways, from driver's licenses to regulation of speed to direction and flow of traffic. Congress and the state legislatures recognized the public safety and health threats posed by the technology of automotive transportation, even as they recognized the dramatic benefits of mobility, productivity, and industrialization that the automobile brought with it. Elected government representatives of the people have consistently acknowledged and acted on their sworn responsibilities by assessing the public safety issues at stake and then regulating the technology accordingly.

Perhaps most relevant to the policy issues posed by encryption is the practice, begun by most states about a hundred years ago, of requiring cars to be registered and to bear license plates. More recently, federal law has required all vehicles to bear a vehicle identification number, or VIN. As you may recall, it was the VIN in the Oklahoma City bombing case that led the FBI to the truck rental office at which Timothy McVeigh rented the truck he used. We now recognize that license plates and VIN's afford victims of accidents, victims of car theft, and law enforcement officials with an essential means of identifying vehicles and obtaining information on the movements of criminals. Just as legislatures in the early 1900's acted to manage the risks posed by automotive technology, government leaders today, as the 21st century approaches, must bring the same sensitivity to the need to preserve and advance public safety in the face of encryption in the information age. And such a regulatory scheme, if constructed properly, will, like license plates, have benefits for businesses and consumers as well.

Of course, no analogy is perfect. Computers are not cars, and plaintext recovery is not a speed limit. But my broader point is an important one. The Framers of our Constitution determined that individuals would not have an absolute right of privacy. The Constitution recognizes that there are certain circumstances in which it is appropriate for law enforcement to obtain information that the individual wants to keep private: for example, when a judge finds probable cause to believe that information is evidence of a crime. Decisions as to where that line should be drawn are political and legal ones, not scientific or business ones; they should be made by this Congress and the courts, not by programmers or marketers. Policy should regulate technology; technology should not regulate policy. Just as in the first part of the twentieth century, the law had to take account of the changes in society brought about by the automobile, the law will have to take account of the changes brought about by encryption.

We at the Department of Justice look forward to continuing the productive discussions we have had with this Subcommittee and the Congress on encryption issues. We share the goal of arriving at a policy and marketplace that appropriately balance the competing public and private interests in the spread of strong encryption.

I would be pleased to answer any questions you may have.

Senator ASHCROFT. It is my pleasure now to call the third panel, which includes James J. Fotis, Tom Parenty, and Bill Wiedemann. Mr. James J. Fotis is the executive director of the Law Enforcement Alliance of America. He has a significant prior career in law enforcement. It is my pleasure to call upon him to begin by making remarks.

PANEL CONSISTING OF JAMES J. FOTIS, EXECUTIVE DIRECTOR, LAW ENFORCEMENT ALLIANCE OF AMERICA, FALLS CHURCH, VA; THOMAS PARENTY, DIRECTOR, DATA AND COMMUNICATIONS SECURITY, SYBASE, INC., EMERYVILLE, CA, ON BEHALF OF AMERICANS FOR COMPUTER PRIVACY; AND BILL WIEDEMANN, FOUNDER AND EXECUTIVE VICE PRESIDENT, REDCREEK COMMUNICATIONS, NEWARK, CA

STATEMENT OF JAMES F. FOTIS

Mr. FOTIS. Thank you, Mr. Chairman, members of the subcommittee, for providing me with this opportunity to discuss the important and complex issue of encryption. My name is Jim Fotis

and I am the executive director of the Law Enforcement Alliance of America, more commonly known as LEAA. LEAA is the Nation's largest coalition of law enforcement professionals, crime victims, and supporters, representing over 65,000 Americans. I am testifying today on behalf of Americans for Computer Privacy, a broad-based coalition working to ensure that privacy of American communications is preserved and protected in the information age.

I am also a retired police officer, and as a retired police officer I urge citizens to protect themselves from attack and thefts in a variety of ways, such as purchasing a deadbolt or a high-tech security system for their house or car, or reminding them to park in well-lit lots and beware of their surroundings. I advocate the same protections for their intellectual property and digital files, and encryption is a deadbolt that locks those files.

However, the administration and FBI Director Freeh have stated that encryption poses a threat to public safety. On the contrary, the threat to public safety comes from the lack of encryption. Files that are not secure are ripe for theft and misuse. Without encryption, the electronic networks that control such critical functions as prison records, the air traffic controller system, and public telephone systems would be vulnerable.

Many governmental agencies utilize encryption. If cryptography can help protect nationally critical information systems and networks against unauthorized penetration, it can also support the national security of the United States, as well as the security of individual citizens. The Federal Government should also be interested in helping to defend U.S. business interests against compromises of information or security leaks. The Justice Department reported computer security breaches cost U.S. business and consumers $7 billion a year.

In today's markets, businesses and individuals transmit a considerable amount of confidential information, including items such as financial records and assets, project and merger proposals, medical records, trade secrets, and research and development information through electronic channels. More significantly, U.S. businesses are competing on a worldwide basis, making them potential targets for competitors, foreign governments, or vandals. So if, by using encryption, we can reduce computer theft crimes and lower economic espionage, it is a net gain for law enforcement.

I work with crime victims every day. We have to give them the power to protect themselves against unwanted attack, physical or informational. As a police officer, I swore to uphold the Constitution of the United States, protect its citizens, and enforce its laws. But the current administration's policies fly in the face of our Founding Fathers, running afoul of the 4th, 1st, 5th, and 10th amendments. Since when did we decide our citizens are guilty until proven innocent, because that is essentially what you are saying when you mandate back-door access to their files?

As an officer, I cannot and will not support a policy that potentially victimizes law-abiding citizens. The proposed legislation would require purchasers of encryption to turn over a key to a third party. That third party might be, in turn, ordered to turn that key over to the Government. So much for fourth amendment guarantees, the right of the people to be secure in their persons,

houses, papers, and effects against unreasonable searches and seizures. If we as law enforcement officers needed to search your computer files or read your e-mail, we should have to go through the same procedures as we would for tangible or real property, meaning we would have to show the court probable cause to obtain a search warrant.

Even scarier than the blatant erosion of our fourth amendment rights is the fact that those supporting this legislation have chosen to ignore a report issued by the world's top cryptographers entitled "The Risk of Key Recovery, Key Escrow, and Trusted Third Party Encryption." It stated clearly, "the field of cryptography has no experience deploying secure systems of this scope and complexity," implying such systems involve security risks and could potentially cost billions of dollars.

The 1996 National Research Committee report also warned third-party recovery introduced a system weakness, putting crucial infrastructures at risk, and questioned whether it could actually work on a large scale. As lawmakers and law enforcement professionals, we have a duty to protect, not jeopardize, our constituents' business and private information. But by concentrating too much power in untested key recovery centers, we make the Nation vulnerable to attack by terrorists and abuse by those entrusted with the power.

Now, to answer the question I know many of you are waiting to ask, yes, encryption sometimes provides a shield for some criminal activities. But the simple fact is that more than 500 strong encryption products are readily available and in use around the world. If the administration is trying to prevent criminal access to encryption, then they are too late. We must strive to keep the political debate focused on criminal behavior and criminal punishment and to communicate the shared opinion of most law enforcement professionals that encryption restrictions are not effective crime deterrents.

Meanwhile, state-of-the-art software applications have thwarted an incalculable number of crimes, protecting millions of dollars and thousands of people, as well as giving street cops and departments such as the Delaware State Police fast access to reliable information before they approach a vehicle, house, or suspect, allowing them to accurately assess potentially dangerous situations.

Police are able to connect directly into the national and State databases, police computers, and national crime information computer. Unlike traditional police radio transmissions, information running over these networks is secure, since the system uses encryption that is inherent in their design. In addition to other benefits, this technology allows officers to stay silent, unlike radio transmissions that can be picked up on scanners by people attempting to keep track of police whereabouts; for instance, drug dealers and burglars.

Now, the FBI is going to say that this will mean unbreakable codes, translating into creation of more crime. This is wrong. For preventing sabotage, you need a system that does not have well-known limits or vulnerabilities. If everybody uses the same type of encryption, sooner or later someone will find vulnerability and fig-

ure out how to break it. Therefore, to be safe, you need different systems.

The FBI says it is trying to stop crime. The problem is you can't stop crime by focusing on inanimate objects. You must focus on the criminal. The criminal terrorist or the college hacker is still out there and using the very weapons our Government won't allow us to access. Simply put, you are mandating that criminals outgun us. It is like giving the American public a rubber baseball bat to *fight* a robber with a gun. If you think this is helping law enforcement, you are dead wrong.

Kenneth Dam of the University of Chicago, who chaired the NRC's committee to study encryption policy, said it best in Issues in Science and Technology. "If encryption can protect nationally critical information systems and networks against unauthorized penetration, it also supports national security."

The cold war has ended, but a new war has emerged, a war for control of our new-found infrastructure, and the only way to win that war and protect constitutional rights is to have strong encryption. Let us not allow 1998 to become the start of "1984."

I thank you for the time and I look forward to your questions. Sir, I would like to explain one thing. We have used the term "law enforcement" in here. There are many, many law enforcement groups out there. There are Federal law enforcement groups, and we said that the International Association of Chiefs of Police and many other groups support the proposals by the FBI. What we have to look at it is the fact that these groups depend on much of the funding from the Federal Government and if they came out against these particular types of legislations and statements by the director of the FBI, they may not get the funds that they need to run their department. There are 18,000 departments out there, most of them under 50 men, and those are the people that I am talking about that don't want encryption.

Senator ASHCROFT. Thank you.

Tom Parenty is the director of Data Communications Security for Sybase, Inc. He has been active in the cryptography and computer security field for over a decade, starting with his tenure at the National Security Agency, NSA.

Mr. Parenty.

STATEMENT OF THOMAS PARENTY

Mr. PARENTY. Mr. Chairman, I would like to thank you very much for the opportunity to address you this morning, and also to thank you for the time and energy you have put into understanding a very difficult and complex issue, and also your leadership in addressing the privacy concerns of this issue in this particular hearing. I would also like to thank other members of the subcommittee and committee who are addressing and interested in American concerns of privacy in the information age.

This morning, I am also speaking on behalf of Americans for Computer Privacy, which consists of over 70 companies and 28 associations, as well as the Business Software Alliance which is an association of the leading U.S. software vendors in the United States. We share two basic principles.

The first is we object to any controls, whether through law or through heavy-handed incentives, on the domestic use of encryption. And in spite of the comments made by—and I confess I cannot recall the precise title of the representative of the Justice Department. We are very concerned about the statements that the director of the FBI has made concerning domestic control.

But maintaining the status quo is not adequate, and so we also advocate an immediate legislative solution for relief on the export side so that U.S. companies might be able to compete internationally on a level playing field.

In terms of my own background, I speak to you as somebody who has spent his entire career protecting sensitive information, starting with my time at NSA in the early and mid-1980's when I worked on nuclear command and control systems, to the present where I work with customers who are building applications for the Internet that will process sensitive business and personal data.

If you look at the Internet today, it is a world in which everyone sends postcards, in which the messages are readable by anyone who simply wants to spend the time to look. And while that is fine for a lot of applications, it is encryption that provides the sealed envelopes that make the Internet safe for real business and sensitive personal use. To make this discussion less abstract, I want to talk about two specific applications that are being built by my customers that highlight the privacy concerns that you are addressing.

The first is in our own backyard in New York State, where the New York State Department of Health is building a child immunization program so that whenever a child goes to a doctor's office, a hospital, a mobile clinic, it will be possible to check on the immunization status of that child and if they need a booster or an inoculation, it can be given to them and their records appropriately updated, something that provides a very clear health benefit for the children of the State of New York. If one looks to the other side of the world, the New Zealand Ministry of Health is building an Internet-based system that will link doctors, hospitals, and other health care providers to be able to share medical information about patients throughout the entire country.

It is clear both of these systems provide very, very strong benefit in terms of providing health care to either the children of New York or the citizens of New Zealand. And because of the very significant privacy concerns in both cases, strong encryption will be used, and specifically strong encryption without third-party key recovery.

I could talk to you today about the technological infeasibility of building a key recovery system along the lines that the administration has outlined. I could also tell you that even if such a system could be built, it would be too expensive to manage. But I will leave those discussions for another time. What I will say is that what third-party key recovery does do is it inserts a vulnerability into what could otherwise be a secure system. It inserts a trap door that could be used by unauthorized personnel, by criminals, or in the case of childhood medical records by child predators. And it is something that both in the New York State case and the New Zea-

land case, they made the right decision not to include that vulnerability.

Having worked on secure systems for over 15 years, I can tell you any of the protestations by the administration that there will be legal and technical measures in place to prevent the abuse of that back door, those arguments ring hollow.

It is clear that encryption enhances national security by providing the robustness and safety that is required for all of the critical infrastructures upon which we depend, such as transportation, health care, banking, things like that. It is also the case that encryption, specifically strong encryption without third-party key recovery, prevents crime by keeping sensitive business and personal data safe from abuse, and in the case of the New York State application being able to offer the ability to protect children in the first place.

In conclusion, I would like to recall a story of something that happened to me in college. It was Christmas. It had snowed the night before and I looked out my living room window to where I had parked my car and I noticed, instead of my car, a black rectangle where my car used to be parked. I thought clearly I was mistaken, so I went into my bedroom and then I came back into the living room, expecting that I would actually miraculously see my car.

Well, the police did find my car several days later. It was stolen; it was pushed off a cliff into a gravel quarry. And while I was happy to get my car back in the condition it was, I could not help but think I wish that I had spent more time and energy protecting my car from theft in the first place.

I thank you, Mr. Chairman, for the opportunity to address you this morning.

Senator ASHCROFT. Thank you, Mr. Parenty.

[The prepared statement of Mr. Parenty follows:]

PREPARED STATEMENT OF THOMAS PARENTY

SUMMARY

Strong encryption protects privacy in the information age

As computer users worldwide become more networked, the need for strong encryption to protect electronic information and confidential information becomes ever more important. Information security is critical to the integrity and stability of individuals, corporations, and governments, and cryptography is the keystone of secure distributed systems. Correspondingly, corporations are now demanding 128-bit, not 40 or 56-bit encryption.

Encryption is necessary to prevent crime and to promote America's national and economic security

The interests of computer users, hardware and software companies and privacy groups are not opposed to those of law enforcement and national security. Encryption prevents crime by protecting trade secrets and proprietary informstion, and this reduces economic espionage. Encryption promotes national security by protecting electronic networks that control such critical functions as airline flights, health care functions, electrical power and financial markets which are highly vulnerable.

The administration's key recovery scheme does not meet demands for privacy

A huge bureaucracy will be necessary to manage the Administration's key recovery scheme.

The technology does not yet exist to create and smoothly operate a reliable system of this magnitude and complexity.

Despite widespread claims of international agreements on "key recovery" infrastructures, no such agreements exist today.

Criminals and terrorist groups will avoid using the Administration's key recovery scheme.

Export controls on American products with strong encryption must be modernized

The results of unilateral U.S. export controls on computer software and hardware with encryption are two-fold:

First, the U.S. government has succeeded in delaying the widespread deployment of American products with strong encryption within the U.S. as well as abroad. Why? Because American companies manufacturing mass market products for the world market find it extremely inefficient and difficult to develop, market, and support two versions of their product—one for the U.S. and one abroad. Recently, some companies have had to go down this route or risk losing purely domestic sales. But this does not help customers with global operations and interests who demand the ability to securely interact worldwide. American companies can only offer these customers products with 40-bit encryption!

Second, the U.S. government has succeeded in giving foreign companies a major market opportunity. An on-going industry by Trusted Information System (TIS Study) revealed that as of September 1997, there were 653 foreign programs and products available from 29 countries, 275 of which employ DES. American companies face strong competitive disadvantages overseas and are losing product sales every day because of current encryption export controls.

The time for action is now

Privacy must be assured, crime prevented and national security promoted. U.S. export controls are inhibiting the use of products with strong encryption domestically. They must be immediately updated to reflect technological and international market realities and enable American companies to compete on a level playing field. Domestic controls in any form that have the effect of forcing the inclusion of back doors must be opposed as they will open up our electronic information to unnecessary and potentially harmful vulnerabilities and insecurities, thus posing an even greater risk to our national and economic aecurity.

INTRODUCTION

Good morning. I am Thomas Parenty, the Director of Data and Communications Security for Sybase, Inc., and responsible for all security-related product development for the sixth largest software company in the world.

I want to take this opportunity, Mr. Chairman, to thank you for taking the time to analyze this complex, difficult issue and for your leadership in helping to bring it to the attention of the public. I also would like to thank the others on this Subcommittee, and on the full Committee—especially Senator Leahy who has worked tirelessly on the subject—who have expressed their desire to address the concerns of American citizens about privacy in the Information Age.

I also, at this time, would like to acknowledge the recent overtures of the Administration and their desire to pursue a dialogue with the private sector to arrive at "cooperative solutions". We certainly are always open to discussion—as we have been for six years. But we need policies now that work for American computer users and American computing companies. That is why we are strongly supporting legislative efforts this Congress to affirm the rights of Americans to use and sell whatever encryption they want and to end unwise export controls on American encryption products.

I have been active in the cryptography and computer security field for over a decade, starting with my tenure at the National Security Agency (NSA) in the early and mid-eighties. While at NSA, I worked on internal NSA computer security issues and focused on the formal verification of cryptographic protocols and internal computer security controls for global nuclear command and control networks. Since then in the private sector, I have worked on the security design of operating systems, networks, and database management systems for many customers ranging from U.S. companies to government agencies, including the Central Intelligence Agency, the Defense Intelligence Agency, and the Air Force. Most recently, I have served as an advisor to the President's Commission on Critical Infrastructure Protection, specifically addressing the needs of the telecommunications and banking infrastructures.

My company, Sybase, Inc., is headquartered in Emeryville, California, and is a worldwide leader in distributed, open computing solutions. We provide customers and partners with the software and services to create business solutions for strate-

gic, competitive advantage. These high-performance, end-to-end solutions encompass client/server, Internet and intranet transaction processing, mobile computing, and data mart and data warehousing applications. Sybase's Adaptive Component Architecture™ enables rapid design, development and deployment of distributed multi-tier business applications. Our product lines include Sybase high-performance database servers, distributed data access and connectivity products, and Powersoft® enterprise development tools.

Today, however, I am not only speaking on behalf of Sybase, but also on behalf of Americans for Computer Privacy (ACP), which includes the Business Software Alliance (BSA)[1] and Sybase.

ACP is a new coalition of more than 70 companies and 28 associations representing the financial services, manufacturing, telecommunications, high-tech and transportation sectors, and associations and organizations, including the Eagle Forum, Americans for Tax Reform, and Center for Democracy and Technology. ACP's mission is to ensure that the privacy of all Americans' confidential files and communications is preserved and protected in the information age. ACP opposes new federal restrictions on the use of encryption products in the U.S. and supports the sale of strong U.S. encryption products to customers around the world.

But most of all, I am here today to speak on behalf of the tens of millions of users of American software products. The American software industry has succeeded because we have listened and responded to the needs of computer users worldwide. We develop and sell products that users want and for which they are willing to pay.

One of the most important features computer users are demanding is the ability to protect their electronic information and to interact securely worldwide. Medical records. Employee evaluations. Information about credit cards, Internet sales, and bank accounts. In short, users are demanding the ability to protect the privacy of confidential and sensitive files and communications.

This morning, I want to make four points:

(1) Encryption protects privacy rights in the information age;

(2) Encryption prevents crime and protects national security;

(3) The Administration's key recovery scheme inherently introduces additional vulnerability and insecurity and will not work; and

(4) In order to promote American's privacy, Congress should reject proposals which mandate—by law or heavy-handed incentives or conditions—key recovery and liberalize existing U.S. export controls on American products with strong encryption capabilities.

Strong encryption protects privacy in the information age

As computer users worldwide become more networked than ever before—through private local area networks (LANs), wide area networks (WANs) and public networks such as the Internet—the need for strong encryption to protect their electronic information and confidential business information becomes ever more important. Companies, governments and individuals now realize that they can no longer protect data and communications from others by simply limiting physical access to computers or by maintaining stand-alone centralized mainframes. Yet they understandably do not want to put sensitive information on line without the best assurances that that information will remain private. A recent Business Week poll, "A Look at On-Liners", found that if privacy were protected, 61 percent of those who currently do not go online would be more likely to start using the Internet, and 78 percent of those who already do go online would be more likely to use the Internet more often.

Consider the New York State Department of Health which is developing the New York State Childhood Immunization Program to track immunization records of children. No matter what clinic, hospital or doctor's office a child visits, a doctor or nurse need only pull up that child's records to determine whether he or she ever got the right shot or is due for booster shots. Because of the highly sensitive nature of the information and because the system will catalogue the names and addresses of the state's children, strong encryption is being used (and no key recovery will be incorporated into the system).

Similarly, doctors have noted that if they have access to even limited clinical information about a patient, especially in an emergency situation (such as pertinent

[1]The BSA promotes the continued growth of the software industry through its international public policy, education, and enforcement programs in 65 countries throughout North America, Europe, Asia and Latin America. BSA worldwide members include the leading publishers of software for personal computers, including Adobe, Apple Computer, Autodesk, Bentley Systems, Lotus Development, Microsoft, Novell, The Santa Cruz Operation and Symantec. BSA's Policy Council consists of these software publishers and other leading computer technology companies, including Intel, Compaq and my company Sybase.

drug information, recent lab tests, or radiology results), they could save billions of dollars by not initiating unnecessary or repetitive procedures.

Encryption provides assurances that the people updating medical records are authorized to make those changes. Encryption also assures that the personal information can neither be viewed or modified by unauthorized parties.

So, too, encryption is becoming vital to the banking and financial services industry. Today, cash is distributed electronically; banks clear and settle their funds electronically, as well. PC/Internet banking is quickly emerging as an alternative to in-person banking or even ATM transaction banking. In fact, one global banking firm recently indicated that 80 percent of its transactions worth trillions of dollars are routinely conducted electronically.

The U.S. Government recognizes the threats hackers pose in the new digital world. In fact, FBI Director Freeh testified that "illegal electronic intrusion into computer networks is a rapidly escalating crime problem. White collar criminals, economic espionage agents, organized crime groups, foreign intelligence agents, and terrorist groups have been identified as 'electronic intruders' responsible for penetration of many of America's computer networks. It is estimated that the Pentagon's computers are subject to hackers' attempts 250,000 times a year." Recently, defense sources said approximately 11 Department of Defense sites were attacked—computers which are used to transmit logistics data as well as pay and personnel information. Deputy Defense Secretary John Hamre has acknowledged that DOD recently has undertaken several exercises that confirmed DOD's vulnerability to computer attack in the future.

Information security is critical to the integrity, stability and health of individuals, corporations, and governments. While cryptography is but one element of security, it is the keystone of secure distributed systems. For these reasons, corporations are now demanding 128-bit encryption.

Encryption is necessary to prevent crime and to promote America's national and economic security

The interests of computer users, hardware and software companies and privacy groups, therefore, are not opposed to those of law enforcement and national security. As the blue ribbon National Research Council (NRC) Committee found in its May 1996 CRISIS Report ("Cryptography's Role in Securing the Information Society"), encryption prevents crime by protecting the trade secrets and proprietary information of businesses and correspondingly reducing economic espionage. Encryption also promotes the national security of the United States by protecting "nationally critical information systems and networks against unauthorized penetration."

Thus, the NRC Committee found that on balance the advantages of more widespread use of encryption outweighed the disadvantages and that the U.S. Government has "an important stake in assuring that its important and sensitive * * * information * * * is protected from foreign government or other parties whose interests are hostile to those of the United States."

In 1996 the Computer Security Institute/FBI Computer Crime Survey indicated that our worldwide corporations will be increasingly under siege: over half from within the corporation, and nearly half from outside of their internal networks. We may see many, many hundreds of millions in losses, and we may possibly see the destabilization of a company, the stock market or perhaps even a whole economy.

To counter these threats, corporations "compartmentalize" their critical business information, and strictly control access to these compartments. Not everyone is trustworthy within a company, and it is this security, this compartmentalization, that prevents crimes such as insider trading, leakage of trade secrets, and corporate espionage. Frankly, there is no substitute for good, widespread, strong cryptography when attempting to prevent crime through these networks.

Widespread use of encryption is also necessary to protect the electronic networks that control such critical functions as airline flights, health care functions, electrical power and financial markets which are highly vulnerable. Indeed, the U.S. General Accounting Office in its report issued in May of 1996 entitled "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," found that: Computer attacks are an increasing threat, particularly through connections on the Internet; such attacks are costly and damaging; and such attacks on Defense and other U.S. computer systems pose a serious threat to national security.

Furthermore, U.S. export controls have had the effect of creating an encryption expertise outside the United States that is gathering momentum. Thus, every time research and development of an encryption technique or product moves off-shore, U.S. law enforcement and national security agencies loose. Continuing down their present path will be more harmful to our national security and law enforcement ef-

forts as American companies will no longer be the world leaders in creating and developing encryption products.

The Administration's key recovery scheme does not meet demands for privacy

The Administration's key recovery scheme is too complex and inherently too vulnerable. Technologically, it will not work on the scale required, and users do not want it. Let me explain why.

First, a huge bureaucracy will be necessary to manage the Administration's key recovery scheme

The Administration's proposal assumes that we can effectively accommodate the needs of dozens of governments, thousands of companies, tens of thousands of law enforcement offices, and millions of users. It also assumes that we can handle tens of millions of public-private key pairs and billions of recoverable session keys across thousands of different products. As the number of people using computers and the Internet grows, the number of keys that must be managed will explode. By the end of the decade, a key recovery system capable of accommodating all of the potential users around the world would have to be capable of handling many, many billions of keys. This is a very tall order. The bureaucracy to manage this key recovery system is likely to rival that of the Social Security Administration, the Internal Revenue Service, or the U.S. Postal Service.

Second, the technology does not yet exist to create and smoothly operate a reliable system of this magnitude and complexity

Furthermore, the Administration's proposed key recovery scheme may actually make consumers more vulnerable. Advocates of a worldwide key recovery system conveniently overlook the tremendous technology barriers posed. It is unclear that such a system can be built at all, much less in the next few years. As Novell's CEO, Dr. Eric Schmidt stated, "Perhaps the technology necessary to create such a system will be available in my lifetime; it is not available today."

Cryptography experts report that "secure cryptographic systems are deceptively hard to design and build properly. * * * Very small changes frequently introduce fatal security flaws. * * * [A]dding key recovery makes it much more difficult to assure that such systems work as intended. It is possible, even likely, that lurking in any key recovery system are one or more design, implementation, or operational weaknesses that allow recovery of data by unauthorized parties." (See The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption, A Report By An Ad Hoc Group of Cryptographers and Computer Scientists, May 1997.)

Third, despite widespread claims of international agreements on "key recovery" infrastructures, no such agreements exist today

Bilateral and/or multilateral agreements must be negotiated and foreign governments' rights and responsibilities must be defined before the Administration's key recovery system can be realized. Despite years of insisting that these treaties were just around the corner, the Administration has yet to conclude a single bilateral, much less multilateral, agreement with another government on key recovery. Nor has the Administration outlined any rights or responsibilities for foreign governments requesting access to U.S. decryption keys held by key recovery agents. It is not even clear whether these keys are subject to civil discovery in addition to criminal discovery.

Ministers and business leaders from 30 European nations attending an Internet conference in Bonn, Germany, roundly critized the U.S. key recovery policy that requires guaranteed access for law enforcement. The ministers agreed in the Bonn Declaration that "they will work to achieve international availability and free choice of cryptography products and interoperable services, subject to applicable law, thus effectively contributing to data security. If countries take measures in order to protect legitimate needs of lawful access, they should be proportionate and effective and respect applicable provisions relating to privacy." The German Economics Minister, Guenter Rexrodt, in fact opened the conference by calling for the removal of restrictions on encryption technology. (See "Should Encryption Software Have Limits?," MSNBC Reuters Report and Jack Breibart, "Europeans Hit U.S. Encryption Policy," American Reporter Correspondent.)

Finally, criminals and terrorist groups will avoid using the administration's key recovery scheme

The stated purpose of the Administration's key recovery scheme is to strengthen law enforcement and national security. But it is unlikely that criminals and terrost groups will choose to use a key recovery system that requires them to provide their

keys to third-parties who can, in turn, give them to government officials. At the same time, it is impossible to force criminals to use a key recovery system!

Unfortunately, other similar attempts at forcing key recovery also are fatally flawed. The Secure Public Networks Act, S. 909, as adopted by the Senate Commerce Committee promotes, through the use of heavy handed incentives, the Administration's mandated third party key recovery access. It is a significant step backwards for American consumers. In fact, far from being a compromise, S. 909 is actually worse than the status quo. The bill attempts to set up an extremely complex domestic key recovery system that puts at greater risk the privacy of all Americans. This complex key recovery scheme will inevitably sacrifice business and consumer's security and unnecessarily drastically increase their costs. At the same time, S. 909 does not ensure easy exportability of stronger encryption or otherwise meaningfully relax export restrictions.

Export controls on American products with strong encryption must be modernized

The incredibly dynamic U.S. computer software industry is an American success story. Since 1980, the industry has grown seven times faster than the rest of the economy and today is larger than all but five manufacturing industries. Conservative estimates are that more than 1.2 million people are employed in the software, hardware, and semiconductor industries—with more than half a million people in the computer software industry alone. This economic success has fueled research and development for new generations of products and spurred the creation of numerous market-leading products and choices.

The computer software industry is one of our country's most internationally competitive. Presently, U.S. software accounts for over 70 percent of the world market, with exports of U.S. software programs constituting half of many software companies' revenues. The incredible growth of the industry and of its exporting success benefits America through the creation of jobs, highly-skilled, well-paid jobs, here in the United States.

But, unless the government's export control policy changes, we will lose our competitive advantage. American software companies are still forced to limit the strength of our encryption to the 40-bit key length level set in 1992—despite an Administration commitment at that time to increase key lengths regularly to take into account technological and market developments. Recent regulations from the Administration allow, on a limited company-by-company basis, the export of products with 56-bit encryption capabilities in exchange for proof of commitments to build "key recovery" into future products. However, not only do customers demand encryption stronger than 56-bit, but this license exception is set to expire in December, 1998. Furthermore the Administration has defined "key recovery" in its own terms, not in consumer-driven terms, and so promoted the development of features for which there is no demand. Thus, 40-bits remains the effective level for which easy export is still permitted.

The results of these continuing, unilateral U.S. export controls on American computer software and hardware with encryption capabilities has been two-fold.

First, the U.S. Government has succeeded in delaying the widespread deployment of American products with strong encryption within the U.S. as well as abroad

Why? Because American companies manufacturing mass market products for the world market find it extremely inefficient and difficult to develop, market, and support two versions of their product—one for the U.S. and one abroad. Recently, some companies have had to go down this route or risk losing purely domestic sales! But this does not help customers with global operations and interests who demand the ability to securely interact worldwide. American companies can only offer these customers products with 40-bit encryption!

For example, a U.S. design company which builds highways, bridges, and dams in foreign countries would like to design its projects here in the U.S. and transmit those designs to foreign countries. Unfortunately, because of the sensitive nature of the information, they would have to use strong encryption with no key recovery—which is prohibited by the U.S. government. Thus, those design jobs go overseas where plans can be designed and developed in a safer atmosphere.

Second, the U.S. Government has succeeded in giving foreign companies a major market opportunity

The General Accounting Office concluded in 1995 that sophisticated encryption software was widely available to foreign users on foreign Internet sites. A 1996 Department of Commerce study confirmed the widespread availability of foreign manufactured encryption programs and products. The most widely used encryption pro-

gram, PGP, with over two million users worldwide, uses the Swiss developed IDEA encryption algorithm, with a 128-bit key. An on-going industry study by Trusted Information Systems (TIS Study) revealed that as of September 1997, there were 653 foreign programs and products available from 29 countries, 275 of which employ DES.

In short, U.S. companies can only sell a product that is inferior to the most popular products already available. It is like being forced to sell a car without bumpers and seat belts in a world which demands safer and safer cars. As a result, American companies face strong competitive disadvantages overseas and are losing product sales every day because of current encryption export controls.

CONCLUSION

The time for action is now. Privacy must be assured, crime prevented and national security promoted. U.S. export controls are inhibiting the use of products with strong encryption domestically. They must be immediately updated to reflect technological and international market realities and enable American companies to compete on a level playing field. Domestic controls in any form that have the effect of forcing the inclusion of back doors must be opposed. It is hard enough to do security right when the sole focus is protecting information—it is incredibly more difficult to do so if one is forced to do so in a key recovery climate. Instead, it will open up our electronic information to unnecessary and potentially harmful vulnerabilities and insecurities, thus posing an even greater risk to our national and economic security.

Thank you.

ACP—AMERICANS FOR COMPUTER PRIVACY

MEMBERSHIP LIST

American Automobile Manufacturers Association.
American Conservative Union.
American Electronics Association.
American Financial Services Association.
American Petroleum Institute.
American Small Business Alliance.
Americans for Tax Reform.
Business Software Alliance.
Center for Democracy and Technology.
Citizens for a Sound Economy.
Computer and Communications Industry Association.
Consumer Electronics Manufacturers Association.
Eagle Forum.
Electronic Commerce Forum.
Electronic Industries Association.
Independent Insurance Agents of America.
Information Technology Association of America.
Information Technology Business Center.
Information Technology Industry Council.
IEEE–USA.
Law Enforcement Alliance of America.
NASDAQ Stock Market.
National Association of Manufacturers.
National Retail Federation.
National Rifle Association.
Online Banking Association.
Securities Industry Association.
Small Business Survival Committee.
Software Publishers Association.
Telecommunications Industry Association.
U.S. Chamber of Commerce.
U.S. Telephone Association.
3Com Corporation.
3K Associates, Incorporated.
ACL Datacom, Incorporated.
Acordia Northwest, Incorporated.
Adobe Systems, Incorporated.
America Online, Incorporated.

Asia Pacific Marketing, Incorporated.
Autodesk.
Axent Technologies, Incorporated.
Bokler Software Corporation.
Brooks Internet Software, Incorporated.
Cisco Systems, Incorporated.
Citrix Systems, Incorporated.
Claris Corporation.
Compaq Computer Corporation.
Computer Associates International, Incorporated.
Consensus Development Corporation.
Corel Corporation.
Countrywide Home Loans, Inc.
DBA Springfield CyberLink.
EDS Corporation.
Envision, Incorporated.
Furukawa Information Technologies, Incorporated.
General Instrument Corporation.
Genio USA.
GeoData Solutions, Incorporated.
Goodyear Tire & Rubber Company.
Honeywell, Incorporated.
I.S. Grupe, Incorporated.
I/O Software, Incorporate.
Intel Corporation.
Intellimedia Commerce, Incorporated.
Intershop Communications, Incorporated.
Intersolv, Incorporated.
Intuit, Incorporated.
Invincible Data Systems, Incorporated.
Kellogg Technologies.
Kinesix Corporation.
Lehrer Financial and Economic Advisory Svcs.
Lotus Development Corporation.
MacSourcery.
Mastercard International, Incorporated.
McLellan Software Center, Incorporated.
MeterNet Corporation.
Microsoft Corporation.
Microtest, Incorporated.
Mindscape, Incorporated.
Napersoft, Incorporated.
NeoMedia Technologies, Incorporated.
Netscape Communications Corporation.
Network Associates.
Network Risk Management Services.
Nokia.
Novell, Incorporated.
Now Software, Incorporated.
Oracle Corporation.
Piranha Interactive Publishing, Incorporated.
Platinum Technology, Incorporated.
Portland Software, Incorporated.
ProSys, Incorporated.
Rail Safety Engineering, Incorporated.
Raycom Data Technologies, Incorporated.
ReCor Corporation.
Rockwell International.
RSA Data Security, Incorporated.
Santa Cruz Operation, Incorporated.
Secure Computing Corporation.
SkillsBank Corporation.
Storage Technology Corporation.
Sun Microsystems, Incorporated.
Sybase, Incorporated.
Symantec Corporation.
Taft Development Group.
Ultimate Privacy Corporation.

Visa International.
Wyatt River Software, Incorporated.

Senator ASHCROFT. Bill Wiedemann is the founder and executive vice president of RedCreek Communications, Inc. RedCreek, another in the long line of Silicon Valley success stories, began operations in July 1996 to address the growing demand by corporations for more comprehensive network security solutions, especially in the Internet market.

It is a pleasure to call upon you, Mr. Wiedemann, and to invite your testimony before the committee.

STATEMENT OF BILL WIEDEMANN

Mr. WIEDEMANN. Thank you, Mr. Chairman. Thank you for providing me with this opportunity to testify in front of this subcommittee today. What I would like to do is just summarize my already submitted testimony for 5 minutes, if I could.

Encryption is a subject of vital importance to the U.S. economy. I have been supporting the U.S. Chamber of Commerce and other groups in Washington throughout 1997 and will continue to do so in the future. Strong encryption is a tool that enables people and businesses to communicate securely. U.S.-based companies are currently the leaders in this technology. Current export restrictions foster foreign suppliers of encryption solutions. The Internet facilitates communication between individuals and businesses. Strong encryption from preferred U.S. suppliers enables individuals and businesses to take advantage of the low cost and wide availability of the Internet as a communication medium.

What I would like to do is talk about basically two points in my submitted testimony, and that is privacy that is afforded through strong encryption, and also meeting the needs of law enforcement through strong encryption.

Currently, we have the ability to export 40-bit encryption to all but seven embargoes countries. 40-bit encryption is not perceived to be strong enough by worldwide corporate customers. I think all of us can remember how safe we felt when our parents gave us our first lock for our bicycle. It was probably four tumblers with numbers between 0 and 9 on each dial. We felt safe and secure because our parents told us that we were safe as long as you didn't let anyone know the combination.

Your first day at school, somebody unlocked your bike and took it for a ride before locking it back up. How did they do this? What they did is simply try every possible combination. It probably took them less than 15 minutes to do that on those 4 tumblers. Industry standard trusted encryption can only be broken using this same brute force type of technique; in other words, trying every key.

It is commonly understood that a 40-bit key can be discovered by trying all the possible combinations in about a week using several hundred computers. A 56-bit key, which is 2 to the 16th or 64,000 times as many possible combinations as a 40-bit key, would take 64,000 times longer or 64,000 times as many computers as a 40-bit key. However, a 56-bit key is still not believed to be strong enough. A 128-bit key is commonly believed to be the length of the key necessary to assure privacy of personal and corporate communications. That is why 128-bit is the approved key length for finan-

cial transactions. However, the U.S. Government currently restricts general export of data privacy encryption to 40 bits.

What I would like to talk briefly about is how we can use strong encryption to enable law enforcement to do their job. As I said, the existing export policy has prevailed to date due to U.S.-based law enforcement professing that these controls are necessary to enable them to pursue criminal activity.

Let us suppose that there were a 40-mile-per-hour speed limit on exported automobiles. Would this enable law enforcement to better pursue criminal activity? Certainly, we would all agree that this would not assist law enforcement, as automobiles are available overseas that can go faster than 40 miles per hour. Yet, law enforcement continues to indicate that a 40-bit restriction on the export of encryption—that that should be the restriction even when stronger encryption is available overseas and enables them to pursue criminal activities.

However, as I mentioned up front and in my submitted testimony, there are several ways to give law enforcement the protection they require and allow corporations to use and deploy strong encryption which, of course, enables their use of the Internet for worldwide secure corporate communications.

Hewlett Packard, as an example, recently obtained U.S. Government approval for their VerSecure technology allowing U.S. suppliers to ship 128-bit strong encryption products overseas. The reason that the Hewlett Packard approach was approved is that exported products are shipped with what is called dormant encryption. The encryption product provides no encryption until it is enabled by a foreign entity or government. Thus, it not only helps with the export of encryption from the United States, but also helps those countries that are trying to restrict importation of certain types of encryption. Foreign countries that have been already approved by the United States Government include the United Kingdom, Australia, Denmark, France, and Germany.

Law enforcement's desire is to recover data by methods that are afforded them today by wiretaps. Any method of data recovery by law enforcement should use the currently established legal practices for obtaining permission to install a wiretap. If the desired data is encrypted for privacy, the wiretap would need to be installed at a point where clear or unencrypted data is available. This is a very simple location. In our example, it would be just inside of our box which, of course, is where clear data is available.

Another method for keeping strong encryption products out of the hands of criminals is to allow the sale of strong encryption only to recognized companies because, of course, they are not the criminals, and then require them to take precautions in the deployment of solutions.

In summary, strong encryption is a tool that enables people and businesses to communicate securely. U.S.-based companies are currently the leaders in this technology. Current export restrictions foster foreign suppliers of encryption solutions, and current proposals to deploy key recovery or other data recovery systems here in the United States would also only further foster foreign suppliers of these solutions.

Thank you.

[The prepared statement of Mr. Wiedemann follows:]

PREPARED STATEMENT OF BILL WIEDEMANN

Mr. Chairman and members of the Subcommittee, thank you for providing me with this opportunity to testify before you today. Encryption is a subject of vital importance to our industry.

PRIVACY AND POLICY

Privacy is considered a fundamental right by all citizens of the United States. Our government has always fully protected this right, whether we are communicating in our homes, through the postal service or over the telephone network. A new communications medium, the Internet, has emerged as the preferred, or certainly a very commonly used, infrastructure. Today we can send email to friends, customers and business colleagues. We do this because it is easy, it allows us to compose our thoughts, and it provides us with a record of the "dialogue."

We can also use the Internet as an infrastructure to conduct commerce.

1. How many of us have bought something on the Internet?

2. Those that haven't yet bought something on the Internet, how many would if they could be assured that it would be safe, secure and private?

Well I am here today to tell you that it is safe, secure and private to communicate and conduct business over the Internet. Software programs are available that enable our existing email and browsers to perform the necessary functions of privacy that make our messages and transactions secure. A major reason individuals in the United States are not using the Internet for ordering products and services is they are not informed that the security of their credit card number is guaranteed by their credit card supplier.

Current policy does not allow U.S. companies to sell data privacy solutions, unless the encryption is 40 bits or less. U.S.-based companies use strong encryption for communications within the United States and Canada but are prevented from using the same products with strong encryption when their communications go outside the United States. The exportable versions contain encryption that is reduced to 40 bits. Therefore, to securely communicate on a global basis, companies obtain a strong encryption add-on from a foreign supplier.

Law enforcement has indicated that the 40 bit export restriction helps them to apprehend criminals. It only hinders the use of these enabling Interent technologies because companies are forced to use foreign suppliers rather than the preferred United States encryption solutions that are contained in the U.S. versions of Interent email and browser products.

Controls on the export of encryption technology, the technology that enables us to attain privacy over the Internet, have curtailed this market and have left some with a felling that the Interent is not yet safe for communications and transactions. A most important fact is that it has only curtailed the use of security solutions. It has not stopped it. Talented engineers and resourceful entrepreneurs in overseas countries have designed plug-ins and add-ons to our favorite email and Internet browser programs. I am sure many of you have seen the articles and quotes from these foreign companies hoping the U.S. government does not change its policy of restricting the export of strong encryption. This restrictive policy is what created and sustains their business. As I said earlier, security is not a problem today for email because foreign companies have solved the problem. The current U.S. policy accomplishes nothing to help law enforcement apprehend criminals. It only curtails the use and therefore growth of the market because global users of these enabling business solutions would prefer not to have to install and support these foreign add-ons for their oversight users.

INTERNET GROWTH

While commerce will grow from $8 billion in 1997 to over $300 billion in 2002 and the number of email users, currently 50 million, doubles every 3 months, an even bigger growth opportunity is the use of the Internet for corporate networks. The Internet will drive the interconnection of corporate offices, remote/mobile users, and business partners. The advantages of the Internet, widely available connections, and low cost access are big expense control and productivity drivers for corporate America. Remote and mobile employees can now telecommute with unlimited access to their corporate resources for as little as $20 dollars per month. Corporate offices can be interconnected for monthly costs that are less than half of other wide area network technologies.

A corporate network based on the Internet is possible because of two things:

1. A widely available quality network.
2. Strong encryption to ensure privacy.

Without strong encryption corporations would not consider putting their private information on the Internet. Strong encryption also provides an impenetrable boundary between the hackers on the public Internet and the users and data on a corporation's private network.

Enterprising companies have recognized this opportunity to provide strong encryption and thereby facilitate secure corporate communications over the Internet. RedCreek recognized the shortcomings in current security solutions and set out to design next generation products. Previous solutions were too slow, too bulky, too costly, and were based on proprietary technology, due to the lack of interoperability standards. U.S. companies such as RedCreek have responded to the need for high performance, small size, low cost, standards-based solutions. Due to this progress in security solutions, companies such as AT&T, MCI, and Sprint can now provide secure corporate connectivity over the Internet.

The availability of a quality network and high-performance security solutions are enabling the explosive potential for the Internet as a corporate networking solution. However, corporations must have the opportunity to obtain strong encryption from a U.S. supplier to address their global networking needs. Today corporations are forced to use foreign company solutions for their overseas locations. As the revenue from security products is handed to foreign suppliers, the current market leading position of U.S.-based companies like RedCreek is jeopardized.

PRIVACY THROUGH STRONG ENCRYPTION

Currently we have the ability to export 40 bit encryption to all but seven embargoed countries. Forty bit encryption is not perceived to be strong enough by worldwide corporate customers. Do you remember how safe you felt when your parents gave you your first lock for your bicycle? It was probably four tumblers with numbers between zero and nine on each dial. You felt safe and secure because your parents told you that you were safe as long as you didn't let anyone know the combination. Your first day at school somebody unlocked your bike and took it for a ride before locking it back up. How did they do that? What they did is simply try every possible combination. It probably took less than 15 minutes.

Industry standard trusted encryption can only be broken using the same "brute force" method of trying every key. It is commonly understood that a 40 bit key can be discovered by trying all possible combinations in about a week using several hundred computers. A 56 bit key is 64,000 times as many possible combinations as a 40 bit key. Therefore a 56 bit key would take 64,000 times longer or 64,000 times more computers than a 40 bit key. A 128 bit key is commonly believed to be the length of key necessary to assure privacy of personal and corporate communications. While 128 bit is the approved key length for financial transactions, the US government currently restricts general export of data privacy encryption to 40 bits.

Financial institutions and U.S.-based companies can use 56 bit data encryption for their overseas offices, however, this is still well below the accepted minimum of 128 bits for data privacy. Consequently users who desire to take advantage of the benefits of these technologies must buy products with unrestricted strong encryption for deployment in the United States and Canada and use foreign suppliers for their overseas offices and partners. Companies such as Timestep in Canada, and Radguard in Israel are not restricted and are shipping solutions that are alternatives to the currently superior solutions available in the United States.

MEETING THE NEEDS OF LAW ENFORCEMENT

The existing export policy has prevailed to date, due to US-based law enforcement professing that these controls are necessary to enable them to pursue criminal activity. Suppose there were a 40 mph speed limit on exported automobiles. Would this enable law enforcement to better pursue criminal activity? Certainly this would not assist law enforcement as automobiles are available overseas that can go faster than 40 mph. Yet law enforcement continues to indicate that a 40 bit restriction on the export of encryption, even when stronger encryption is available overseas, enables them to pursue criminal activities.

Law enforcement's current proposal is to allow 56 bit encryption to be shipped outside of the United States as long as they can get access to a copy of the encryption key. How many of us would be willing to make a copy of our house key and car key available to U.S. and foreign governments without prior notification of the use of our key? Many people consider this type of government access to our encryption keys an extreme invasion of privacy.

However there are ways to give law enforcement the protection they require, and allow corporations to use the strong encryption, which enables the use of the Internet for worldwide corporate communications. Hewlett Packard recently obtained U.S. government approval for their VerSecure technology allowing U.S. suppliers to ship 128 bit strong encryption products overseas. The reason that the Hewlett Packard approach was approved is that exported products are shipped with "dormant" encryption. The encryption product provides no encryption until it is "enabled" by a foreign entity or government. Foreign countries that have been approved by the United States include the United Kingdom, Australia, Denmark, France, and Germany.

Law enforcement's desire is to recover data by methods afforded them today with wiretaps. Any method of data recovery by law enforcement should use the currently established legal practices for obtaining permission to install a wiretap. If the desired data is encrypted for privacy, the wiretap would need to be installed at a point where clear (unencrypted) data is available.

Another method for keeping strong encryption products out of the hands of criminals is to allow the sale of strong encryption only to recognized companies and then require them to take precautions in the deployment of the solutions.

SUMMARY

Mr. Chairman and members of the Subcommittee, privacy is a fundamental right of all people. Strong encryption is a tool that enables people and businesses to communicate securely. U.S.-based companies are currently the leaders in this technology. Current export restrictions foster foreign suppliers of encryption solutions.

The Internet facilitates communication between individuals and businesses. Strong encryption, from preferred U.S. suppliers, enables individuals and businesses to take advantage of the low cost and wide availability of the Internet.

Senator ASHCROFT. I want to thank all of you for your testimony.

Mr. Parenty, tell me about your company's experiences with current encryption controls and whether they harm your international competitiveness.

Mr. PARENTY. Certainly. I would like to talk on two points, one of which is, especially in the last 6 months, any conversations with customers overseas—and this covers a wide variety of respected industries—have said that they would not purchase any products from us unless we were able to provide a solution that included 128-bit encryption.

We tried to work with the administration in their key recovery plan that would allow the temporary export of 56-bit encryption and our experience was that the rules changed underneath us as time went by, so that it was impossible for us to make any business plans based on what the Government would allow us to do. And so our personal experience with the KMI exception program showed us that it was not something a business could participate in. We also found that the ability to export just 56-bit DES overseas is not something that satisfies any of our legitimate customers' needs.

Senator ASHCROFT. So is it your view that the exceptions that are available are unworkable?

Mr. PARENTY. That is absolutely correct.

Senator ASHCROFT. Our Government has allowed export of up to 128-bit encryption for financial matters. Are these financial concerns more important or entitled to greater protection than other kinds of trade secrets, in your judgment?

Mr. PARENTY. In my judgment, they are not. And in point of fact, when one thinks of the kinds of information that are transmitted over electronic networks, specifically the Internet, there are many very valuable, sensitive kinds of information above and beyond simply an electronic funds transfer.

I had mentioned specifically examples in the medical industry. It is also quite true that American companies that have subsidiaries and partners overseas have a very significant issue with respect to protecting their intellectual property. And there is a very strong concern and worry about any kind of system that would involve giving a foreign government escrowed access to keys because there is a lot of experience that we have with foreign governments using their intelligence agencies in economic espionage against U.S. companies.

Senator ASHCROFT. Mr. Fotis, I want to be clear on your testimony. You are saying that, contrary to the previous FBI assertions, not all the law enforcement agencies across the country are against the capacity of people to use robust encryption?

Mr. FOTIS. That is correct, Senator. In 1988, I developed one of the first internal automation systems in Nassau County. It is being used by the Nassau County police and about 35 other police departments in New York. If this had been in effect, we would have had to give a back door to the FBI to get into our system not only from the companies' standpoint, but from the police departments' standpoint. There are sensitive investigations that go on in every small to medium police department and they do not want the FBI or other Government agencies to be able to get into their encrypted records.

Senator ASHCROFT. Mr. Wiedemann, you suggested perhaps, if I am not mistaken, that if we were to have robust encryption, we could limit it to only well-established, large companies. Was I correct in hearing you say that?

Mr. WIEDEMANN. Yes, that is certainly one proposal. I don't believe that law enforcement believes that this should be restricted use to respectable companies, you know, Fortune 1000 or recognized worldwide companies. And as long as they were able to control the deployment of that in a secure fashion, that could restrict it being used by criminals.

Senator ASHCROFT. Certainly, in the computer industry companies come and go from the list of respectable, top companies pretty rapidly. Are there any startup companies that might have a need for robust security that would parallel or equal the needs of the well-established companies?

Mr. WIEDEMANN. Certainly, virtually all companies have the need for—many of our customers, in fact, are small companies that are desiring to communicate in a secure fashion using these data networks.

Senator ASHCROFT. Mr. Parenty, we don't have any limitation on the use of encryption in the United States now, is that correct?

Mr. PARENTY. That is correct, yes.

Senator ASHCROFT. So you can use 128-key encryption, very robust encryption in the United States?

Mr. PARENTY. That is correct.

Senator ASHCROFT. And every company can, or every individual could here at this time?

Mr. PARENTY. Yes.

Senator ASHCROFT. Why is it that it doesn't appear that a lot of people are using it? You know, you talk about the Internet being a postcard now, but if we were to have certain kinds of encryption

available internationally, it would somehow become a sealed envelope. Well, for most people who don't really go around the world on the Net, but just go to talk to their kids in Chicago or what have you, there does not seem to be much utilization of encryption. Can you explain that?

Mr. PARENTY. It is something that when you think about the use of encryption, the first thing that one should keep in mind is in some sense the best and most effective encryption is absolutely transparent to the end user. And one very good example of the role of encryption in daily lives that people may not be aware of is ATM machines. When I use my ATM card and get money from the bank, encryption is being used to protect my financial situation.

And it is the case that even for individuals who are perhaps just using the computer for sending e-mail to their child in college, there is a significant amount of personal, financial, medical, spending-pattern, consumer-oriented information that is on the networks today. And it is something that I think it is incumbent upon policymakers to ensure that that information is adequately protected.

Senator ASHCROFT. Thank you, Mr. Parenty. I want to thank the members of the panel. We have one more panel to move through today and I am eager to get their testimony. They are a panel of constitutional experts. I am grateful for all of your participation.

Mr. PARENTY. Thank you.

Senator ASHCROFT. Let me thank each of you for coming. I would welcome any presentations of written documents, in addition to your spoken testimony, and I will begin immediately with the introduction of Professor Kathleen Sullivan, the Stanley Morrison Professor of Law at Stanford Law School. She is a noted expert on constitutional law, including the first amendment and criminal procedure. Her prominence in the field is illustrated by the fact that the 20th Century Fund selected her as a contributor to the "New Federalist Papers: Essays in Defense of the Constitution."

Professor Sullivan, thank you for coming. We would be pleased to have your remarks.

PANEL CONSISTING OF KATHLEEN M. SULLIVAN, PROFESSOR, STANFORD UNIVERSITY SCHOOL OF LAW, STANFORD, CA, ON BEHALF OF AMERICANS FOR COMPUTER PRIVACY; RICHARD A. EPSTEIN, PROFESSOR, UNIVERSITY OF CHICAGO LAW SCHOOL, CHICAGO, IL, ON BEHALF OF AMERICANS FOR COMPUTER PRIVACY; CINDY A. COHN, McGLASHAN AND SARRAIL, SAN MATEO, CA; AND TIM D. CASEY, CHIEF TECHNOLOGY COUNSEL, MCI COMMUNICATIONS CORP., WASHINGTON, DC

STATEMENT OF KATHLEEN M. SULLIVAN

Ms. SULLIVAN. Thank you very much, Mr. Chairman. Thank you for the opportunity to testify before the subcommittee and thank you for your interest in this very important topic about privacy in the digital age.

Mr. Chairman, as you stated in your opening remarks, the Framers created a world under our Constitution in which privacy is very substantially protected. It is protected because the Framers established a world in which the Government may not engage in general

searches, may not engage in dragnets, no matter how effective they may be for law enforcement. The Framers created a world in which we may speak freely and protect our privacy freely, unless and until there is particularized cause to think that we are doing something wrong.

The first amendment has been interpreted by the Supreme Court to say that the Government may never ban an entire category of speech, may never ban an entire medium through which we speak. It may simply regulate particular instances of speech that create danger, such as the proverbial shout of "fire" in the crowded theater. And under the fourth amendment, the Court has been quite clear that we cannot have general searches.

Now, the problem with any system that would mandate that those of us who encrypt the messages we send or store on the Internet—any system that would require us to turn over the key to third parties inverts that world that the Framers so carefully put in place. It would say not that all speech is presumed free unless and until it poses a danger, but it would say, rather, all speech is presumed potentially relevant to the Government and we are going to collect it and store it all in a way that makes it more accessible to the Government in advance.

Now, the administration says, "Well, don't worry. We will have to have particularized cause at the later point when we try to obtain information from the storehouses that we have required you to set up with these third parties." And, with respect, I would like to submit that, as the chairman's remarks pointed out, that is not enough. Particularized cause later is not enough to cure the problem of a general search at the outset, and let me talk about a few examples to try to make this point clear.

Imagine that the Government were to say we all have to install surveillance cameras in our houses. We won't turn them on, of course, the Government says, unless and until we have reason to think you are doing something wrong. But I think we all would sense that we have suffered a tremendous loss of privacy just by creating that potential for surveillance which, of course, might be intercepted by the wrong parties as well as by the Government.

If the Government were to say, "Well, now that we have smart clothing and smart jewelry, all of you are required to wear computerized jewelry that we could turn on at any point when we wanted to study your movements; we would only turn on this monitoring device, of course, if we thought you were about to do something wrong"—but I think we would sense that we have lost a great deal by even having to wear that jewelry and create that opportunity for the Government.

Or as the chairman pointed out in his opening statement, suppose the Government were to say that we have to file copies of every one of the documents that we produce and would like to keep private, would like to keep between us and the intended recipient, with an escrow agent, with a third party, with a bank or a safe deposit box somewhere. The Government might say, "Well, we are only going to compel those papers from that box we have made you store them in if we think you are doing something wrong." And yet I think we would all agree that we had lost a tremendous amount of privacy up front when we had to give that up.

Now, Justices on the Supreme Court have recognized this principle many times, none perhaps so eloquently as Justice Harlan, who wrote in a 1971 opinion that the fourth amendment is designed not to shield wrongdoers, but to secure a measure of privacy and a sense of personal security throughout our society; that is, for all of us who are law-abiding citizens and corporations.

Now, Justice Harlan in that opinion said that, of course, if the Government simply listened to us all the time, we would give up that sense of what he called the spontaneity and frivolity that characterize our sense of life when we think we can keep our life private among the people we want to speak to and not open to the outside world.

So the first point would be that the world the Framers set up is that Government needs particularized suspicion. It can't run a general search at the outset and assure us that, of course, it will never use this data until later. The privacy loss happens at the outset.

The second point I would like to stress—and these points are elaborated in my written testimony and I am grateful if the chairman would admit that to the record.

The second point I would like to make is that contrary to the position that Mr. Litt took on behalf of the administration, the regulation of encryption is the regulation of speech. It is a mistake to think that a new technology changes the basic principles of the first amendment. It would be a mistake, for example, to say that a telephone call is not protected by the first and fourth amendments just because it travels through electrons rather than on a paper that is carried by horseback, and the Supreme Court said it wouldn't make that mistake when it protected our telephone calls under the fourth amendment in 1967.

I think we would all recognize that if the Government tried to regulate print and ink instead of regulating a newspaper, that would implicate the first amendment. I think we would all see that if the Government said you have to send your letters by postcard or in transparent glacine envelopes, that would limit speech in a way that would implicate the first amendment. And so the fact that people send messages in bits and digits does not affect the fact that these regulations would affect speech.

And finally, and in closing, cooperative solutions are not necessarily constitutional. Cooperative solutions have the potential to be coercive. Cooperative solutions that try to use the Government's leverage and buying power and procurement power and regulatory subsidy power in order to extract responses from industry may, in fact, implicate the Constitution. The Supreme Court has repeatedly recognized that sometimes conditions on funding and conditions on contracts can be unconstitutional when the Government goes too far, when it seeks to use its leverage over a private contract, for example, to tell its contractor what the contractor can do with his or her or its own suppliers. Further elaboration is in the written testimony.

Thank you for the opportunity to make these remarks.

Senator ASHCROFT. Thank you very much, Professor Sullivan. I appreciate the remarks and they are helpful.

[The prepared statement of Ms. Sullivan follows:]

PREPARED STATEMENT OF KATHLEEN M. SULLIVAN

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to testify before you on the constitutional concerns raised by various proposals by the Administration, the Federal Bureau of Investigation, and some members of Congress to restrict the use of data encryption on the internet, in particular by requiring those who make or use encryption technologies to turn over their digital keys to third parties in order to preserve ready access by government to the encrypted information. Whether or not such proposals would, if enacted, be struck down by the United States Supreme Court, the very least that can be said is that they pose serious risks to the liberty and privacy values embodied in the First Amendment's protection of the freedom of speech and press, the Fourth Amendment's protection against unreasonable searches and seizures, and the Fifth Amendment's protection against compelled self-incrimination. These constitutional costs should be factored carefully into consideration of any legislation governing key recovery.

Whatever disagreements might divide participants in this controversy, all can agree upon certain starting points. First, it would seem beyond reasonable dispute that instantaneous global communication over the internet has great benefits to offer both to our commercial marketplace and to our marketplace of ideas, and that the ability of those who use the internet to maintain some degree of privacy in their communicationa is essential to maximizing those benefits. Various polls have suggested that privacy is a very important issue to users of the internet; for example, a recent Harris poll reported in Business Week found that 78 percent of users would be more likely to use the internet if its privacy protections were more secure. If the internet is to fulfill its vast potential, then citizens and corporations must be confident that sensitive information that flows over the internet—from the transmission of credit card numbers, medical records and trade secrets to the discussion of views critical of government—will be shielded from unwanted eyes and ears. Privacy with respect to sensitive information and unpopular opinions is as basic an American value in the fast-paced information age of the late twentieth century as it was at the time the Constitution was framed. By enabling secure lines of communication, encryption allows privacy to retain its historical meaning even in an era of changing technology.

Second, all can agree at the same time that the use of robust encryption poses some risks as well as benefits. The use of encryption by criminals or terrorists, for example, may well make it more difficult in particular instances for the government to protect law-abiding citizens, corporations or the government itself against threats to personal, business, or national security. In the absence of mandatory key recovery systems, law enforcement officials can decode encrypted information only if they can obtain voluntary or compelled cooperation from the sender or recipient, seize a key from someone else to whom the sender or recipient has voluntarily or accidentally entrusted it, or deploy superior computing power sufficient to break the code by the mathematical equivalent of brute force. Of course, law enforcement officials retain, even in the digital age, a wide array of traditional methods of surveillance as well as considerable power to search for, seize, or compel production of communications in plaintext. Nonetheless, it is understandable that some law enforcement officials would prefer additional access to encrypted information through the back door of key recovery.

But, third, any such backdoor key access undeniably has formidable costs as well as benefits. There can be little doubt that universal third-party key escrow, if mandated, would reduce the degree of privacy we would all enjoy if we could use strong encryption without turning over keys to outside intermediaries. The creation of a massive, complex system of key escrow intermediaries that are not controlled by users would dramatically multiply the opportunities for information to be transferred into the wrong hands through the mistaken or fraudulent release of keys. It would also lead to the concentration of valuable data in centralized databases that would be far more inviting and vulnerable to targeted attack by criminals than would more decentralized systems of key maintenance. Backdoor decryption would also, by design, compromise privacy in relation to government. No matter how benignly motivated, and even if subject to threshold requirements of judicial approval, government use of key recovery will inevitably be prone to risks of error. By thus compromising the privacy and security that could otherwise be obtained through strong encryption, mandatory key escrow would likely have at least some deterrent effect on the use and growth of internet communication.

Once these initial propositions are established, it becomes clear that the question before this Subcommittee is whether the actual gains to effective law enforcement from mandatory key access justify the considerable costs to constitutionally pro-

tected privacy interests that it would entail. Concerns about crime and terrorism will always seem overriding in the abstract. But legislation does not operate in the abstract. If mandatory key access is likely to be highly porous, then criminals will evade its strictures and it will fail to serve the vital but generalized government interests asserted by key access advocates. On the other hand, for ordinary law-abiding citizens, mandatory key access does much that turns traditional constitutional liberties on their head. The method involved in mandatory key escrow—namely, compromising every citizen's liberty and privacy in order to make it easier for government to intercept or capture the unlawful few—is the reverse of our usual procedures under the First, Fourth, and Fifth Amendments. Usually we allow citizens a wide berth for freedom unless and until their exercise of liberty threatens to harm others or the state. Thus, no matter how laudable the generalized law enforcement goals at issue, mandatory key access also involves extremely serious constitutional tradeoffs.

1. Freedom of Speech and Press. The First Amendment provides in relevant part that "Congress shall make no law abridging the freedom of speech, or of the press." Of course, the right to speak is not absolute; government may regulate speech to prevent particularized and imminent harms, such as the stampede that might be caused by the proverbial shout of "Fire!" in a crowded theater, or the violence that might ensue from a speaker's face-to-face provocation of an edgy mob. But the story of free speech protection in the twentieth century consists very largely of the Supreme Court's increasing insistence that entire categories of speech may not be categorically or prophylactically presumed in advance to be dangerous and therefore regulable. Rather, outside of certain narrow areas of unprotected speech such as obscenity, extortion or blackmail, the government is constitutionally required to be put to its proof, case by case, that a particular instance of speech is so likely to be seriously harmful as to justify its regulation. See, e.g., *Brandenburg* v. *Ohio,* 395 U.S. 444 (1969).

The Supreme Court likewise has held repeatedly that government may not impose a total ban on an entire medium of expression in which willing speakers and listeners otherwise would engage. For example, government may not ban all leafleting in the public square, all door-to-door solicitation for charitable causes, or all posting of signs on privately owned residences by their owners. As the Court recently noted in a unanimous decision, its "prior decisions have voiced particular concern with laws that foreclose an entire medium of expression" because, even if such laws do not discriminate against particular ideas, they "can suppress too much speech." *City of Ladue* v. *Gilleo,* 512 U.S. 43 (1994). First Amendment suspicion is understandably raised by any law that, like a total medium ban, will predictably reduce the quantity of expression in society.

Mandatory key escrow proposals contravene these traditional approaches to free speech because they in effect impose a total ban on a medium of expression—the medium of securely encrypted digital communication—based merely on generalized predictions of dangerousness. Because some unescrowed encrypted communications might amount to a crime or provide evidence of a crime, all unescrowed encrypted communication is forbidden. This reverses the usual presumption that all categories of speech and all media of expression should be permitted unless and until a particular instance of speech is shown to be imminently likely to cause serious harm.

Mandatory key escrow is in considerable tension with another aspect of our First Amendment tradition as well: By compelling the maker and/or the user of encryption products unwillingly to disclose how to decrypt coded information, it arguably violates the right not to speak that has long been read as an unspoken corollary of the right to speak. Government generally may not make us speak against our will, whether by pledging allegiance to a flag, bearing a slogan we find offensive on our automobile license plates, or turning over part of our property to serve as a bulletin board for our critics. Similarly, government generally may not force us to disclose our identity when we engage in otherwise protected expression. The Supreme Court has long held, for example, that civil rights activists and others who risk retaliation for their important but unpopular speech may not be made to sign their pamphlets or disclose their organizational membership lists merely because doing so might make it easier for government to monitor for subversion or fraud. See *Talley* v. *California,* 362 U.S. 60 (1960); *NAACP* v. *Alabama,* 357 U.S. 449 (1958).

The Court recently reaffirmed this right against compelled disclosure of identity in a decision invalidating, on First Amendment grounds, a criminal ban on unsigned literature in a referendum campaign. In that decision, *McIntyre* v. *Ohio Elections Commission,* 115 S. Ct. 1511 (1995), both Justice Stevens and Justice Thomas emphasized that an author's decision to remain anonymous is part of a venerable tradition that stretches back to the nation's founding era: the Federalist Papers them-

selves were written under the pseudonym "Publius" and countered by anti-Federalist tracts written under such pseudonyms as "Cato," "Brutus," and "the Federal Farmer." To be sure, internet users of encryption technology seek to keep private the content of as well as the signature on their documents. But a generation that included Paul Revere as well as Madison, Hamilton and Jay undoubtedly understood that content ("one if by land, two if by sea") no less than authorship sometimes needs to be encrypted.

It is no answer to such concerns that the proposed third-party key escrow systems, unlike earlier proposals for government key escrow, require disclosure of decryption keys not to the government but rather to private parties chosen by each speaker. The Supreme Court has invalidated, for example, a requirement that charitable solicitors disclose the amount they spend on overhead to the private parties from whom they seek donations. See *Riley* v. *National Federation of the Blind*, 487 U.S. 781 (1988). As the Court emphasized in *Riley*, what matters is not to whom the disclosure is directed, but whether the government has "mandat[ed] speech that a speaker would not otherwise make." Mandatory key escrow by definition does just that.

Nor is it necessarily a sufficient answer to such concerns that mandatory key escrow aims not at the message but at the vehicle by which it is expressed—that is, at the equivalent of the envelope rather than the letter. For the Supreme Court has often admonished that regulation of conduct that facilitates speech triggers the First Amendment no less than regulation of the speech itself. For example, government may not prohibit payment for solicitation of signatures on ballot petitions or the receipt of honoraria for off-duty speeches and articles by government employees, because such regulations decrease incentives to engage in speech even if the speech itself may be engaged in by other means. See *Meyer* v. *Grant*, 486 U.S. 414 (1988); *United States* v. *National Treasury Employees Union*, 513 U.S. 454 (1995). Similarly, the Court has been just as willing to invalidate a selective tax on paper and ink as to invalidate a selective tax on a newspaper itself. See *Minneapolis Star* v. *Minnesota Commissioner of Revenue*, 460 U.S. 575 (1983). Requiring escrowed key encryption—like requiring that letters be mailed in glassine envelopes—would surely discourage speech as effectively as a tax or regulation on the underlying speech itself, and thus call for heightened scrutiny under the First Amendment.

Finally, any provision that conditions the right to make or sell encryption software upon the government's prior approval of that software's key recovery capabilities might raise familiar First Amendment concerns about prior restraint. Assuming that computer code, like scientific or musical notation, free verse or abstract painting, counts as speech as much as does a political tract or the daily news, such preclearance requirements, like any system of speech licensing, creates the danger that the exercise of administrative discretion will tend to give inadequate protection to interest in freedom of speech. See *generally Bernstein* v. *United States*, 974 F. Supp. 1288 (N.D. Cal. 1997).

2. Protection From Unreasonable Search and Seizure. The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." It also provides that "no Warrants shall issue, but upon probable cause" and "particularly describing" the objects of search or seizure. The reasonableness and warrant requirements help to ensure that, under our systems of government, law enforcement officials will not engage in dragnets or general searches, no matter how useful they might be in facilitating occasional access to evidence of crimes. The reason is, of course, that a general search also sweeps in countless other innocent transactions of daily life, thus diminishing the privacy and security enjoyed by law-abiding citizens. As Justice Harlan once wrote, the Fourth Amendment "is designed not to shield 'wrongdoers,' but to secure a measure of privacy and a sense of personal security throughout our society." *United States* v. *White*, 401 U.S. 745 (1971) (Harlan, J., dissenting). Mandatory key escrow bears a troubling resemblance to a general search, exacting a significant surrender of privacy and security in the absence of any initial particularized suspicion.

The interests protected by the Fourth Amendment, which extend beyond "persons, houses, papers and effects" to all aspects of our lives in which we have "reasonable expectations of privacy," were not frozen in time in the eighteenth century. Those interests may well alter or expand with the advent of new technologies. In *Katz* v. *United States*, 398 U.S. 347 (1967), for example, the Court easily found a twentieth-century telephone call be the functional equivalent of eighteenth-century "papers," and thus determined that the government's warrantless use of a modern electronic eavesdropping device was just as problematic under the Fourth Amendment as redcoats rummaging through one's drawers. Fourth Amendment protections ought likewise extend by analogy to the internet: Just as one who shuts the door to a phone booth and pays for a phone call may reasonably expect that the content of his phone

call will not be intercepted, so one who encrypts the content of a transmission over the internet and carefully secures the key has taken socially reasonable steps to maintain the confidentiality of his communication.

To be sure, we do not maintain reasonable expectations of privacy in those aspects of our lives that we voluntarily reveal to potential uninvited onlookers. For example, the Supreme Court has held that the Fourth Amendment does not constrain government searches of open fields that would be visible to hunters passing by and airplane pilots flying overhead, or of garbage bags placed on the curbside where their contents would be readily accessible to scavengers and the trash collector. See *Oliver* v. *United States,* 466 U.S. 170 (1984); *California* v. *Greenwood,* 486 U.S. 35 (1988). But the Court has never held that the government is presumptively entitled to access to anything more than we choose voluntarily to reveal, or risk revealing, to the world at large. We are not normally expected to grant easements of access to the government to areas of our lives that we have generally shielded from meaningful public view.

Mandatory key escrow inverts these usual presumptions by requiring that citizens take affirmative steps to facilitate government surveillance. Imagine if government, for similar reasons, requested us to live in glass houses, conduct all our conversations loudly and exclusively in English, carry all our personal belongings in clear plastic bags, or keep all of our possessions in unlocked cabinets or drawers. Most Americans would no doubt be deeply troubled by such laws. Government may not bootstrap its way out of Fourth Amendment constraints simply by outlawing methods for preserving privacy that would otherwise be considered reasonable within the broad contours of our customs and traditions.

Or suppose that government, under laws more closely analogous to mandatory digital key escrow, ordered that copies of all personal papers be deposited in safe deposit boxes in private banks, or that a duplicate of every set of house keys be kept with an insurance agent, in order to facilitate ready later access by law enforcement officials. Such methods, much like the regular conduct of general searches, would seriously compromise the individual privacy and security that we all enjoy, not just that enjoyed by would-be criminals.

It makes little difference that one is compelled to turn over one's keys, as an initial matter, to private parties rather than to the government. The compromise to individual security and privacy remains much the same. Nor is it plausible to suppose that no government search or seizure really occurs until government approaches a key escrow agent for the key—at which point there will be a warrant, a court order or at least enough particularized suspicion to make the government's action reasonable. Any particularized suspicion that might be thought to justify key recovery at a later time cannot cure the problems caused by the generality of the initial sweep.

Imagine, for example, that government required that we all install surveillance cameras inside our homes—while promising to turn them on only upon particularized suspicion. Or suppose that government were to require that we wear computerized jewelry that could be programmed by government to monitor our movements—but only if government comes to suspect that we are about to do something illegal. And suppose further that government turned on the cameras or activated the silent beeper without any specific notice to use akin to the ancient common-law requirement of knock-and-announce. In such settings, government's promise that it would activate its enhanced capacity to invade our privacy only if it accurately suspected us of some wrongdoing would hardly be enough to assure us that it would never make a mistake or single us out for some other less relevant reason. It is the very purpose of the Fourth Amendment to shift the risk of such error to the government.

Finally, proponents of mandatory key recovery might argue that it presents no greater Fourth Amendment problems than does the requirement that digital telephones be configured to allow the government to wiretap conversations. This analogy is inapt. Telephone users necessarily surrender some control of their communications to telephone companies, who in turn can be, and historically have been, forced to surrender access to the government; by contrast, the internet makes possible unmediated communication between speaker and listener in which the users at all times can maintain exclusive control of the decryption keys. Mandatory key recovery thus would force internet users to make a copy of a key they never would have lost control of in its absence. Moreover, telephone interception applies to ephemeral communications, while mandatory key recovery gives government potential access to a much broader realm of stored data.

3. Privilege Against Self-Incrimination. The Fifth Amendment provides, among other things, that no person "shall be compelled in any criminal case to be a witness against himself." This privilege against self-incrimination helps prevent government from plundering the defendant's own mind for assistance in convicting him of a

crime. But to trigger the protection of this clause, a communication must simultaneously be testimonial, incriminating and governmentally compelled.

The contours of the privilege as it applies to compelled surrender of encryption keys are controversial, but one thing is clear: Mandatory key escrow would operate to defeat any Fifth Amendment protection that might otherwise attach by disaggregating the elements of any defense. In the absence of third-party escrow, government would have to try to compel individual keyholders to divulge or hand over their keys. Forced recitation of a key from memory, like forced recitation of a combination to a safe, is arguably testimonial, as well as incriminating and compelled. Compulsory surrender of a recorded version of a key might likewise trigger the privilege, at least if the act of production of the key were itself communicative, for example authenticating a document or attesting to the defendant's connection to the message that key enables the government to decrypt.

But the Fifth Amendment privilege could be bypassed altogether if government could compel production of a key by a third-party escrow agent rather than from the user of the key. The user's surrender of the key at the outset is compulsory, but not at that time either testimonial or incriminating. The user's creation and encryption of any particular message is voluntary, not compelled. And even if a key enabling decryption of a particular message is incriminating to the user, its compulsion from the third-party escrow agent does not amount to testimony by the user. In short, the Fifth Amendment privilege might sometimes protect the papers of a defendant from compulsory production by the defendant, but not from compulsory production by a third party, and at a minimum, the same logic would appear to apply to decryption keys.

Mandatory key recovery thus helps to work an end run around the protections of the Fifth Amendment privilege against self-incrimination. Normally it is up to individuals to decide whether to increase the risk that their documents—or, in this context, their decryption keys—will ultimately be surrendered to the government by transferring those documents to third parties. Mandatory key recovery takes away that choice.

4. The Problem of Futility. Even clear infringements of fundamental constitutional rights can sometimes be justified if they are sure to serve compelling government interests. Prevention of crime, terrorism and threats to national security are undoubtedly compelling interests. But it is very far from certain that domestic encryption controls—even in tandem with existing or future export controls—will be genuinely effective in preventing such dangers. For the skilled user, strong encryption will inevitably be available for import from foreign sources. And the availability of strong encryption from foreign sources can be expected to increase further to the extent that domestic encryption controls drives software design talent overseas. Furthermore, high-tech criminal activity can be expected to cultivate its own encryption expertise, and those who are undeterred by the general criminal law are unlikely to comply with third-party key escrow requirements. While standardization of key recovery-based encryption products thus may enable detection and deterrence of criminals at the lower end of the expertise scale, mandatory key recovery is far less likely to do the same for the most sophisticated and dangerous criminals or terrorists. The lower the expected utility of a particular technique of law enforcement, the less justifiable its adverse impact on our general sense of privacy and security.

5. Unconstitutional Conditions. The constitutional concerns raised above would not evaporate if government sought to achieve key escrow through use of its spending power, rather than through direct regulation. The Supreme Court has long held that there are limits to how much regulatory leverage government can obtain through its market participation. Across a range of constitutional areas, the Court has held that government's power to dictate the terms on which its own resources may not be used to dictate the terms on which its contracting partners or grantees may use their own resources. For example, a grant of a public broadcasting subsidy does not entitle government to bar all editorializing by the recipient, even if such speech is supported by private funds. Nor may government dictate to a public employee what income he may derive from speech activities he undertakes in his spare time. Similarly, the government may impose key recovery requirements on computer products and internet services that it purchases for its own (presumably non-classified) use. But that does not necessarily entitle it to impose such requirements on its suppliers in their dealings with private customers.

To the extent that network externalities require those who do large amounts of internet business with the government to standardize their products for both public sector and private sector markets, there is a real danger that government procurement conditions will operate in fact as regulatory conditions extending far beyond

the scope of a government contract. The significant temptation for overreaching in such a setting calls for the exercise of considerable governmental self-restraint.

Conclusion. Privacy is a basic and traditional constitutional value served in overlapping ways by the First Amendment's protection of anonymous speech; by the Fourth Amendment's protection of our persons, houses, papers and effects and their modern equivalents; and by the Fifth Amendment'a protection of knowledge we commit to memory and decline to divulge to anyone else. Mandatory key access would undermine all three protections. It would reverse the usual constitutional presumption that we are free until we pose a threat of material harm, presuming instead that all securely encrypted internet communications are potentially appropriate targets for government access. Such an inversion of our constitutional order might be justified if mandatory key escrow really could keep criminals and terrorists at bay. But a complex non-user-controlled key access system is likely to be both easily evaded by high-tech criminals and increasingly vulnerable to their predations at the expense of ordinary citizens. Under such circumstances, mandatory key access should be rejected.

Senator ASHCROFT. Richard Epstein is the James Parker Hall Distinguished Service Professor of Law at the University of Chicago Law School. He has written widely on a variety of constitutional issues too numerous to mention and has authored perhaps the most influential modern work on the takings clause.

It is my pleasure to call upon Professor Epstein at this time.

STATEMENT OF RICHARD A. EPSTEIN

Mr. EPSTEIN. Thank you very much. I would like to depart a little bit from my written statement to comment on some of the points that were made by the Justice Department and try and put it in some sort of a larger context.

Senator ASHCROFT. Thank you.

Mr. EPSTEIN. I think the basic context that one has to examine in all of these particular disputes is a world in which there are always two kinds of errors. In some situations, it turns out that individuals are deprived of privacy which they ought to be able to keep, and in other cases individuals engaged in criminal activities will be able to maintain privacy that they ought to be able to lose.

The great question and the reason why we have such long hearings is that there is no set of social institutions that can drive either of these kinds of errors to zero, and the effort to insist or to pretend that there is a way in which you can guarantee that you will be able to achieve all of your ends without necessarily compromising any of the desires of other individuals is, on purely a priori grounds, simply a fiction that cannot be sustained.

I think the great mistake in the Justice Department's position is that they assume that they can continue to guarantee the same safety with weak encryption—that is, encryption that is subject to the back-door key—as they can without it. The only question that one has to ask is not whether that is possible. It is not. The question that one has to ask is whether or not the sacrifices and safety that come by virtue of the installation of the trap door are worth it in terms of the law enforcement benefits that can be gained. I think the answer to that question, on balance, has to be regarded as no.

The simplest way in which I would like to put this is to ask yourself who is likely to be more responsive to the ability to evade these kinds of regulations, criminals who do not register with the Government and who are not known in advance or large and major corporations whose every activity is subject to Government regulation

and whose ability to operate, as it were, off the books would subject them to severe sanctions of all kinds and descriptions.

The simple point, I think, is that to the extent that we have a world in which there is explicit regulation with key recovery and similar devices, we will have a world in which the criminals will not play. They will find some ways to go overseas. They will take pretty good privacy methods that are out there already and use them. They will make sure, in effect, that they will engage in a variety of deceptions that will render the system of regulation essentially ineffective.

In addition to this, it seems to me that we have to recognize that the system itself can break down. The moment you start to install third-party key recovery systems, you have to ask a lot of questions which are not answered by the Government at this point. Who is going to be a trusted key operator? Who is going to, under these circumstances, pay these people in order to provide the services that they render? Is it going to be paid for by the Government? Is it going to be paid for by the individuals who are forced to turn their keys over under these circumstances? How are these parties going to work and what are going to be the consequences in the event that there is a slip-up so the data in question in going to be lost through inadvertence or through theft?

These are constant questions, and it is simply not sufficient, in my judgment, to say that appropriate regulations can be used in order to handle these problems. Before one wants to embark on these kinds of surveys, you have to know what these regulations are, not simply take a promise that they could be made that way.

I have looked at enough of the reports by technical people to believe that what they say is, in fact, correct. At the moment you introduce two keys to any particular document, it is not a question of market savvy. It is a question of an impossibility theorem. You cannot make something which has two keys to it as safe as something which has only one key. You cannot make something which responds to the demands of law enforcement which would be as good as a voluntary system of key recovery that responds only to the demands of the customer who happened to purchase that thing in the first place.

Now, with all of this said, the balance, in effect, is going to be extremely important in the way in which you think about first amendment and fourth amendment and other kinds of rights in question. Whenever one sees the word "unreasonable" before anything, you know that some kind of a balancing test is going to be involved. And if what I said is correct that the gains to law enforcement will be subject to massive evasion by criminal efforts, but the losses to private individuals engaged in lawful activities will be very substantial, then it seems to me that the reasonable balance is put in the direction of saying stay the hand of Government under these circumstances.

We were told, of course, however, by Mr. Litt that regulation is all-pervasive, and his remarks he concludes with a discussion of how it is that the United States does not ban automobiles, but nonetheless subjects them to various kinds of extensive regulations, some of which, I might add, off the record, I deplore. But that is not the point that we are worried about here. The question we are

worried about here is whether the analogy will work as a constitutional or as a business matter, and I submit to you that it fails on both of these grounds.

The first point that one has to recognize is that to the extent that you are talking about the regulation of automobiles on a public highway, you are talking about the kinds of activities which under current Supreme Court doctrine receive the lowest level of scrutiny and protection. To the extent, on the other hand, that you are dealing with privacy and other kinds of first amendment speech and interest, you are dealing where there is either intermediate or strict scrutiny. To show that there is pervasive legislation in an area of rational basis review is not to show anything about what happens where the level of review becomes much more stringent. So under these circumstances, if you look at the regulations, it seems to me that they surely fail.

In addition, the kinds of regulations that one has asked for in an area more sensitive are far more sensitive than the sorts of regulations that you had in the other areas. To give but a simple point, if the only thing you could do with respect to computer records was to have license tags on them, then the Government would be able to see that there is an undecipherable message which is sent out by company xyz. It would not be able to get the stuff in question.

So what happens is the Government gets the wrong standard of scrutiny, and then what it does is it demands the wrong level of invasion relative to that level of scrutiny. It may be that there are certain kinds of license tags or identification numbers or something else that could be worked out, but a strong key is far more intrusive than any form of regulation that is demanded with respect to the automobile.

This is not a case where if you want to go on the highway, you would have to file in advance with the Government your travel plans before you are allowed to use the roads. Over and over again, one has said that the monopoly that the State has over the public means of communication does not allow it to impose whatever terms and conditions it sees fit on individual citizens. That is true with respect to the highways going back to the 1920's. It ought to be true of the Internet today.

Thank you.

Senator ASHCROFT. Thank you, Professor Epstein.

[The prepared statement of Mr. Epstein follows:]

PREPARED STATEMENT OF RICHARD A. EPSTEIN

A World of Clashing Imperatives. The issues before the Subcommittee raise the inescapable tension between two sets of vital concerns, both of which deserve constitutional recognition. On the one hand lies the need of all Americans to preserve privacy and confidentiality of information essential to their personal lives and their professional businesses. No one can doubt the huge volume of sensitive information that travels across the internet—medical records, financial information, trade secrets, intellectual property. The immense value of that information will be compromised or lost if allowed to fall into the wrong hands. Yet by the same token, no one can doubt the legitimate needs of law enforcement officials at the federal, state and local levels to monitor the high tech criminal activities that threaten the security of this nation, the liberty of the citizens within it, and the security and safety of the property they own. It would be irresponsible to offer testimony before this Committee that slights the strength and validity of either interest.

Acknowledging the importance of both ends sets the stage for analyzing the current controversy: legislative proposals that mandate, often through some form of a

key escrow or key recovery system, mandatory government access to private encryption of sensitive information. With weighty interests on both sides, the proper accommodation all boils down to a single set of relevant considerations. What are the costs and benefits of the various systems that step up public surveillance over private information transmitted over the internet? To see why, just consider for a moment the position of private users of the internet if they knew to a certainty that the present proposals for mandatory government access were foolproof, that is, that they always worked only as intended. Given that assumption, government law enforcement agencies would only obtain private encrypted information when able to show probable cause that the information would assist them in detecting, preventing or solving a crime. The information in question would be strictly limited to these purposes. This fail-safe system could never be misused by public authorities; and the creation of the trap door method of entry into the system would never compromise to the slightest degree the ability of strong encryption to keep its messages from fanatical terrorists, criminal elements, computer hackers, rogue governments or other undesirables who wanted to seize it for their own advantage. Finally, all the governments of the world could adopt this fail-safe system as well as the protections for individual privacy guaranteed by the Fourth Amendment. Satisfy these strict conditions, then every private firm that now strongly opposes the many variations for mandatory public access to encrypted information might testify on behalf of the proposal. They would benefit from the increased security obtained from superior law enforcement efforts, and they would experience no diminution in the security and efficacy of their private telecommunications. The world would be devoid of nettlesome trade-offs, and delicate risk calculations.

But these companies have formed a massive alliance to protest the proposals of the Clinton Administration, the Department of justice and the Federal Bureau of Investigation to introduce any system of mandatory access into every private communication made over the internet. It is not that these companies are opposed in principle to vigorous criminal law enforcement that protects the sensitive personal information and trade secrets of their own businesses and their millions of customers. It is because they reject this optimistic scenario on both practical and theoretical grounds.

Practically, they insist that the advanced technology needed to operate a system of key recovery on a massive scale is not available; theoretically, they believe that advances in computer technology alone will never be able to overcome the inherent risks associated with the operations of this system no matter how many design safeguards the federal government seeks to build into the system. It is clear, almost as a matter of first principle, that the more complex a system of transmission of encrypted information must be, in serving multiple ends, the greater the likelihood its design will compromise its ability to achieve it stated mission—the secure transmission of sensitive information over the internet. Technical complexity does more than increase the costs of transmission: it also creates weaknesses in structure that can be exploited by the very criminal parties whose activities the government wishes to curtail by its mandatory access programs. The technical report of the Ad Hoc Group of Cryptographers and Computer Scientists, "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption" (May, 1997) demonstrates this conclusion beyond any shadow of a doubt. Any trap door system increases the risk that someone else will be able to find, duplicate or manufacture the key to the encrypted information. The trap door places enormous operational trust in personal security systems that government officials must develop to handle massive amounts of data and billions of separate keys. That logistical key-control center exposes the entire system to the risk of a common-mode failure which in turn becomes the obvious target point for terrorist and criminal elements: blackmail, deception, impersonation can all be focused on a single known end. No complex administrative program advances only its stated ends. Each creates unwanted incentives that set in motion complex forces that are only imperfectly perceived when the program is first introduced. Social theorists often warn of the unintended (and counterproductive) consequences of purposive action. That warning must be heeded here. Lawful individuals and firms will be trapped by Byzantine requirements, imperfectly executed; criminal and terrorist elements will hone in on ways to evade or subvert the complex structures at hand.

What is so distressing about the current hearings is that high law enforcement officials are so inattentive to the specific objections raised against the programs of mandatory access that they refuse to acknowledge the risks their own initiative creates. The letter of Attorney General Reno, FBI director Freeh and six other high criminal law enforcement officials in the Clinton administration to members of Congress on July 18, 1997 embodies this unsound approach. The letter notes:

"As we move from the plaintext world to an encrypted one, we have a critical choice to make: we can either (1) choose robust, unbreakable encryption that protects commerce and privacy but gives criminals a powerful new weapon, or (2) choose robust, unbreakable encryption that protects commerce and privacy and gives law enforcement the ability to protect public safety. (Emphasis added.)"

With respect, the choices offered miss the entire point. As stated, the letter assumes that a system of perfect enforcement can be implemented; how else could it be said (1) that strong encryption without mandatory access only protects criminals but confers no additional advantage on the private individuals and firms that use it, and (2) that the system of encryption with mandatory access remains "robust and unbreakable" when every known expert in the area stresses the heightened vulnerabilities to which this system exposes its users. Any candid analysis of the tradeoffs must recognize that a system of robust, unbreakable encryption also reduces the targets for criminal and terrorist activities and thus their rate of occurrence. Any accurate overall assessment must also recognize that any key escrow system compromises, perhaps fatally, what would otherwise be a robust and unbreakable system of encryption. It is perfectly proper for the Attorney General, the Director of the FBI and their key law enforcement officials to point out the advantages of the system they champion. It is wholly improper for them to pretend that it contains no real disadvantages. The proper choice between difficult alternatives is not advanced by any communication that pretends that the relevant trade-offs simply do not exist.

The Constitutional Implications. Thus far I have stressed the practical and operational risks inherent in any system of mandatory access. I believe that this background information not only goes to the legislative wisdom of the Clinton Administration proposals but also to both its constitutionality and impact on property rights. It would be idle for any opponent to mandatory key access to claim before this Subcommittee the fatal nature of the many constitutional objections lodged against the proposed legislation. The complex nature of the legal issues mirrors the complexity of the technical problems of implementation. The most that can be claimed in the absence of authoritative determinations by our Supreme Court is that the proposed statute travels on a collision course with many of the guarantees of individual liberty found in our Constitution. I think that it is the obligation of this Committee to make its own independent assessment of these constitutional objections before deciding whether or not to recommend the passage of any legislation that contains the mandatory access provisions sought by the Clinton Administration and the Department of Justice. In so doing, I believe that it is perfectly proper for this Committee to refuse to recommend passage of the legislation if it finds these Constitutional objections severe and weighty even if it is uncertain whether the Supreme Court would be certain to strike that legislation down. It is in that spirit that I shall examine the proposed legislation against two vital Constitutional guarantees: the forth amendment's protection against unreasonable searches and seizures, and the fifth amendment's protection against the taking of private property without just compensation. "Unreasonable Searches and Seizures:" The Fourth Amendment reads:

"The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized."

The jurisprudence on this clause has been vast, both in the courts and outside, but a few salient features of the clause deserve special mention. First, the coverage of the amendment extends to all the "people," and thus is directed toward the comprehensive form of government activity contemplated by all mandatory access programs. Linguistically, the coverage of "persons, houses, papers and effects" does not capture perfectly the nuances of the information age, but it takes very little tugging to see their contemporary relevance. In particular, "papers" are protected not because they are blank, but because of the sensitive information they contain. These records and information do not lose their protection because they are stored digitally or transferred electronically, only to regain that protection when printed out in hard copy. The Supreme Court had no difficulty in deciding that telephone calls and private conversations could not be tapped and overhead without regard to the requirements of the fourth amendment, and the same logic surely applies to the electronic information involved in this area.

A similar approach should be taken to the question of whether the imposition of a mandatory access program should be regarded as a search or seizure within the meaning of the fourth amendment. The precise question has not been answered by current Supreme Court law, but its case law provides us with some clues as to the proper direction of the analysis. The constitutional protection against searches and seizures is not limited solely to the protection against government trespasses, al-

though these are always included. Rather, the protection extends as well to a reasonable zone of privacy that also protects individuals from some nontrespassory forms of snooping. Here it is sometimes said that all individuals are entitled to a reasonable expectation of privacy, which is fine so far as it goes, but should never be construed to allow the government to dash all expectations of privacy by announcing in advance its intended program of state surveillance. The term "reasonable expectations" is meant to serve as a further barrier to government intrusions of all sought. These expectations cannot be defeated by the facile observation that so long as one knows that the government is about to snoop, then no one has any reasonable expectation of privacy. Rather the right way to look at expectations is to note that the Constitution insures the protection of a reasonable zone of privacy even against the determined efforts of government to undermine it.

With that said, the cases here do raise some difficult issues of principle that are not fully resolved under the case law. Thus far the litigated cases have all involved situations where the government has gained information at the same time that it has been taken from its owner. A recovery key system, however, does not take things from the private citizen and give them to the government. Rather it sets the stage for their easy transfer at some other time, either with or without a warrant. In dealing with the protection of individual liberties, I believe that constitutional guarantees are triggered by what the individual citizen has lost. The escrowed key was taken at the direction of the government and put into the hands of an agent of its own choosing. If the same thing were done with a second key to a safe or a front door, could it be said with a straight face that the government has not "seized" the key from its owner simply because it did not rummage through his papers? And once the key is seized, could one deny that it has compromised the integrity of that safe or house?

I take it as beyond question that the surrender of the escrow key surely compromises the integrity of its owner's sensitive information. That surrender also makes it easier for the government to gain actual possession of that information at some later date, especially since a government official can turn the escrow key in the computer lock without the knowledge or cooperation of the individual whose information is being gathered. A key that is taken for one purpose may easily be used for another. Indeed if the information is never introduced as evidence in court, the invasion of privacy could take place free not only of judicial sanction but even of judicial knowledge. Under these circumstances it seems idle to say that the fourth amendment does not apply because government has not taken the individual's papers or effects. I think the protections of the fourth amendment are triggered when government action takes the key and compromises the natural defenses that ordinary owners have, just as it would be triggered if the government were authorized to place hidden microphones in every telephone, microphones that could be turned on only with the assistance of some responsible third party.

The next question is whether this seizure of the escrow key should be regarded as unreasonable under the fourth amendment. Here the government puts forward only generalized concerns with international terrorism or organized crime to justify its massive invasions. Yet it must concede that the number of actual transmissions which it is entitled to intercept constitutes only a minuscule fraction of those to which it gains potential access. The insecurity of the mandatory access program, however, ripples through each and every transaction for which the government receives its hidden key, so that the government faces a heavy burden to explain why that initial seizure should be regarded as reasonable. In this case, it can get no help from the warrant requirement, for the generalized insistence on mandatory access does not remotely demonstrate any "probable cause" of criminal activity. Nor could any warrant possibly issue for receiving such a key in the absence of any particular description of the transmissions that will be intercepted.

The entire system of preestablished key recovery reads like in indirect evasion of the individual safeguards normally afforded under the fourth amendment. The system introduces a massive system of potential surveillance. It cuts out the notice and knock provisions that must be satisfied before a warrant could be executed. It vests vast powers in third-party agents who have neither the incentive nor knowledge to contest any government intrusion. It presupposes uniform good faith by public officials and overlooks the major costs of even a tiny number of official misdeeds or mistakes. The proposed mandatory access system should be condemned therefore "as an unreasonable search and seizure." The Senate should not give its blessing to a scheme of such dubious constitutionality. Instead it should encourage law enforcement agencies to adopt other methods of investigation and surveillance, and to enter into cooperative agreements with major firms in the internet business to expedite the request for information when the more exacting warrant requirements are met.

Fifth Amendment Takings. At this point, I think that it is also appropriate to express my concerns in another area: should the government have to pay compensation to those persons whose confidential information has been compromised by leaks from government sources? The relevant text in this context is of course the fifth amendment protection against takings which reads in full:

"Nor shall private property be taken for public use, without just compensation."

The command of the fifth amendment is best analyzed as though initially it raises ordinary questions of tort and property law. The government insists upon the receipt of certain keys for its own benefit. It is therefore as though the government were the bailee of these keys, for its own use. The law of bailments has long dealt with the allocation of the risk of loss when property bailed is stolen or lost. Those analogies help inform the constitutional inquiry into the law of takings.

Initially, let us suppose that some third party steals a key from the government and uses it to unlock information that causes great private loss. Everyone agrees that the third party should in principle be subject to criminal and civil sanctions, assuming that he could be apprehended. But the law is equally clear that the party who received the key—its cyberspace bailee—may frequently be found liable when apprehension of that third party is not possible. And no cases ever hold that the deliberate actions of a third party necessarily insulate the bailee from liability for its antecedent conduct: the tort law generally has routinely acknowledged that more than one party could be a proximate cause of a given plaintiff's property damage.

Just that analysis applies here. The law of bailments often apportions the risk of liability in accordance with the pattern of benefits derived from the bailment relationship. In this case the transaction is done over the objection of the private party and without its consent: the benefit is for the public at large, and the risk is to the private party. Under those circumstances, traditional common law doctrine places the risk of loss from third party interventions squarely on the bailee (here the government) whose actions has increased the risk or hazard of the bailor's (here the individual or firm's) loss by its own conduct for its own advantage. The standard always holds the government liable for ordinary negligence, and for routine cases of theft or loss may impose strict liability as well. But by no stretch of the imagination does the private law confer total immunity for all misconduct on the bailee.

In looking over these various draft bills, all of them deny private parties any recourse for liability against the government on the one hand or the third party escrow agents on the other. This sheer assertion of public will does not of course make the losses disappear; and it will encourage the government officials to overuse and underprotect its own key system since the government receives total immunity from the financial (let alone social) consequences for the damaging loss of commercial and personal information that could easily take place.

It is, moreover, a fair question to ask whether the government's efforts to insulate itself from the consequences of its own actions generates potential liability under the takings clause: the government has taken the key and compromised the contents of the files: why insulate it from the loss that it concentrates on some particular individuals for the benefit of the public at large? To be sure, the government may raise a number of technical legal defenses on its own behalf. It may argue that it has not taken the information in question when the improper disclosure is directly done by a third party, and thus take refuge behind a highly restrictive reading of the takings clause. The government takes a key that operates a dam and places it in the hands of a third party. The key is stolen, the dam is opened, and a citizen's land is flooded. Should the government be entitled to deny that it has taken property when it is clearly liable under ordinary tort law for the property interests it has compromised or destroyed? Should the government claim that the disclosure of confidential information only amounts to a tort and not a taking when no one has been able to articulate clearly the line between the two? Should the government be entitled to invoke the doctrine of sovereign immunity where its necessity for action rests not on some identified imminent peril or danger, but only on some undifferentiated concern about crime and terrorism not tied to the transaction at hand?

The losses inflicted by government action are real and palpable even if these technical defenses should persuade a court not to require compensation for the private losses of these public programs. But one central purpose of a constitution is to restrain the excessive powers of government, and that is hardly done by immunizing it from liabilities that have long been applied to private persons whose own exposure to risk should, if anything, be less than the governments. (After all, no private party can compel someone else to turn over a back door key for their personal use.) A strong case could be made that the takings clause should in principle apply to deprivations of property brought about by the loss or theft of the government key. It is far from self-evident that the Supreme Court will reject that position when the full risks of the mandatory access program are made apparent to it. It is also clear

that this Committee, with its special concern with property rights generally, should scrutinize the constitutional, legal and moral power of the property claims that stand in the way of the current government initiative.

Unconstitutional Conditions. Thus far I have examined the desirability and constitutionality of direct government proposals to regulate the use of electronic transmissions. A more complete analysis must also take note, however, of the indirect forms of regulation available to the state. The government is an omnivorous user of electronic transmissions. It deals extensively with all sorts of private parties on a direct contractual basis. One concern is that it might seek to impose these conditions by executive order as part of its ongoing contractual relations with major suppliers of internet and electronic services.

In many cases the imposition of conditions under grants or contracts is a routine part of any transaction. Thus no one questions that the government is entitled to specify the quality and quantity of services demanded, the terms of payment, and the time and conditions of its delivery. But just as private parties may from time to time use their power to improperly advance their position in collateral markets, so too government may use its power to extend its influence into ordinary spheres. The federal government has exclusive control over the interstate highway system, and yet no one thinks that it can condition the access of drivers to that system on their willingness to abandon their fourth or fifth amendment rights in unrelated contexts. So it is that it would be wholly inappropriate for the government to stipulate that it would not do business with any firm that refuses in its unrelated transactions to adopt a system of escrowed key recovery.

This possible restriction of strong encryption not only places ordinary individuals and firms at risk, but it also threatens to undermine the appropriate division of labor between the separate and equal branches of government. The question of mandatory access to private communication or electronic transmission is too vexing and controversial to be solved by executive order. It should command the anxious attention of Congress so that any proposal goes through the full deliberative process before its possible adoption. An executive order should be discouraged not only because of its adverse consequences on individual rights, but also because of the threat it poses to the structural safeguards found in our basic constitutional structure.

Export Controls. Last I should mention a few words about the use of export controls as a device to limit the manufacture and deployment of strong encryption devices. In the short run these are likely to inhibit the proliferation of these devices, at least as long as the United States enjoys some technical advantages over the rest of the world. The impact of these restrictions, moreover, should be felt in domestic as well as foreign markets, given the reluctance of domestic producers to make different products to serve different portions of what is ultimately a global market in internet and communications services.

Yet the protection afforded by export controls promises to be short-lived at best. The efforts of the United States to get other nations to go along with its mandatory access programs have failed (ironically even in nations that have no entrenched constitutional provisions). If the United States cannot export its technology to the world, then talent will flow to those nations free of the restrictions that limit United States producers. In the long run, leadership in technology will follow freedom to innovate, so that strong encryption devices will be available throughout the world. Our own futile effort to prevent the spread of these devices will only result in the erosion of our leadership in a potentially booming field of industrial growth. The strategy will be self-defeating in the end.

Conclusion. In making these observations, I want to be perfectly clear that the recognition of constitutional protections always comes at some cost. It could well be in some given situation, the adoption of the mandatory access regime proposed by the Clinton Administration could outperform a technology world in which private parties may continue to use strong encryption devices as they see fit. But the issue before this Committee, and before the nation, should not be decided with reference to a single scenario without reference to other possibilities that seem more likely. A mandatory access provision may also allow foreign terrorists or organized crime to sabotage the very communications system that the mandatory access provisions are designed to protect.

We live in a world with great potential; but it is also a world of great risks. We must do the best that we can to minimize the risks. But that requires us to consider the scenarios in which government regulation does harm as well as those in which it does good, and to make the best and most responsible decision that we can on the strength of all available information. On matters such as these it is difficult to separate the constitutional from the practical considerations, and at this stage in the inquiry, it is far from clear that we should make that separation at all. The various proposals before this Committee on mandatory key access pose far more risks

than they eliminate. The proposal should therefore be rejected both for the risks that it creates for private transmissions of electronic information, and for the dangers that it poses to the constitutional protections for individual liberty that have long helped to keep this nation both free and strong.

Senator ASHCROFT. Cindy Cohn is an attorney with McGlashan and Sarrail, of San Mateo, CA. She served as the lead counsel in *Bernstein* v. *U.S. Department of State,* in which the court held that software code was protected speech and that export regulations violate free speech guarantees.

Ms. Cohn, thank you very much for being with us and we would be pleased to have your testimony.

STATEMENT OF CINDY A. COHN

Ms. COHN. Thank you, Senator. I want to thank the subcommittee for inviting me here today. Although there have been very many hearings and much discussion about cryptography here in Washington, this is the first hearing, I believe, to seek testimony from one of the attorneys directly involved in the legal challenges to the cryptography regulations.

I have been asked here, as you said, because I am lead counsel in the case of *Bernstein* v. *Department of Justice, et al.* The name of the defense agency keeps changing, but at the moment it is Department of Justice. With the help of the Electronic Frontier Foundation, Professor Daniel J. Bernstein has been trying for over 6 years to publish on the Internet a very simple cryptographic computer program which he himself wrote. He has been told that if he does so, he will be prosecuted.

We have argued that American scientists, be they academics, in industry, or hobbyists, should not have to submit their own work prior to publication to faceless Government bureaucrats. This is especially the case when those same bureaucrats have unfettered discretion to bar them from publishing their own work. But that is what the current scheme allows. The Federal District Court for the Northern District of California has agreed with us that the regulations are a violation of the first amendment on their face, meaning that they violate the rights of all Americans and not just Professor Bernstein.

I wanted to take this opportunity to tell you about two other similar cases which are also pending. The first, *Karn* v. *U.S. Department of State,* is here in the D.C. district court. The *Karn* case is the clearest example of the quip often made about the administration's cryptography policy that it is based upon a belief that terrorists cannot type. Mr. Karn was told that although a book containing computer source code could be freely sent abroad, a floppy disk containing the exact same information could not, under fear of prosecution.

The second case, *Junger* v. *Christopher,* is in Cleveland, OH, and is based upon the Government's position that Professor Junger, a law professor at Case Western University, could be prosecuted for teaching a Computers and the Law course in his normal way.

In the *Bernstein* case, we have received three rulings from the district court so far, all of them in our favor. The final ruling in our favor was appealed by the administration, argued in December 1997 before the Ninth Circuit Court of Appeals, and is now waiting

decision. I have attached a copy of the third district court opinion to my written statement for your review. I hope that your staff will take the time to review it, as well as my more full comments in my written statement. The opinion gives a clear and concise statement of some of the key constitutional requirements that any legislation on cryptographic software must meet and a better explanation than I could ever give you about why the current regulations are flatly unconstitutional.

As I mentioned before, the *Bernstein* case challenges the current Government restrictions on cryptographic software on the grounds that they are in violation of the first amendment. Although our case focuses, as it must, on the current regulatory scheme, the analysis would apply as well to most of the proposed domestic restrictions on cryptography, and certainly on any that would restrict or license the creation, distribution, or receipt of cryptographic software. Indeed, the constitutional problems which arise if domestic controls are imposed are even more severe.

I want to tell you a little bit about the doctrines of first amendment law that are raised in the *Bernstein* case and that the district court adopted. The *Bernstein* case focuses on the easiest flaws to see in the current scheme, the lack of procedural protections. The Supreme Court has long held that if the Government wants to institute a pre-publication licensing scheme on speech, it must contain, first, a provision of a prompt decision, no more than two weeks, by the agency; second, a provision that only a court can stop publication. The Government must bring a court action if it wants to stop publication and it cannot simply act administratively. And, third, the Government bears the burden of proof in court. This comes from a seminal Supreme Court case called *Freedman* v. *Maryland.*

I should point out that as much as I would like to take credit for this legal analysis, we were not the first ones to see this problem. In fact, the first people to point out these constitutional problems in the cryptographic regulations were the Justice Department's own Office of Legal Counsel in 1978. You see, the agencies have known for over 20 years that their regulations are flatly unconstitutional and it was their own lawyers who told them so. This is why you rarely hear them mention the first amendment in their presentations to you, or if so, only in brief passing.

The key point in our case and in your consideration of any proposed legislation is that source code is protected expression for purposes of the first amendment. On this point, the administration largely agrees. Let me repeat that. Despite what the Department of Justice representative said here today, in our legal case the administration has not denied that in regulating computer software it is also regulating the expressive activities of Americans. This conclusion, which is obvious to anyone who has ever written or read a computer program, is also consistent with what Congress has repeatedly held. Software is treated as identical to other forms of protected expression in both the Copyright Act and the Freedom of Information Act.

Now, up to this point, everything that I have said isn't just my opinion; it is the opinion of the Federal district court. My legal team and I believe, however, that there are other strong constitu-

tional reasons to prevent the regulation of cryptographic software. I won't elaborate on the ones already ably discussed by Professor Sullivan and Professor Epstein, but there are a couple of additional ones that I would like to bring to your attention.

In addition to procedural protections, the Constitution requires that any regulation which institutes a licensing scheme or any other form of prior restraint must pass the strictest of tests. Even a claim of national security or public safety must be carefully weighed against our fundamental rights and must be supported with hard evidence of direct, immediate, and irreparable harm from the publication of the material, not just conjecture and not just a few frightening scenarios.

Further, aside from prior restraint, a scheme which targets speech on the subject of cryptography and treats that speech differently from speech on other topics must pass the test of strict scrutiny; that is, the regulation must address a compelling Government interest and be narrowly tailored to reach only that interest and no further.

Further, the Government must prove that their restrictions on speech actually meet their goals. This would be difficult in this case, since terrorists, child predators, and drug dealers can simply purchase or download strong German, Swiss, or Japanese encryption software that is freely available all over the United States and the world—over 500 encryption programs at last count. If necessary, as I mentioned before, criminals could even type in or scan one of the many computer programs printed in the books published on this subject.

Neither the current scheme nor any administration-supported so-called compromise scheme proposed so far address these first amendment problems. And even the SAFE bill, which is well-intentioned, fails to contain an assurance of judicial review of any agency decision to prevent publication due to alleged national security concerns, a key element required by the Constitution. SAFE also does not clearly protect scientists such as Professor Bernstein. It only protects those who seek to distribute mass-market software already available abroad. That means that American scientists can no longer participate in the ongoing international development of this vital and important area of science.

As you mentioned before, in our research for this case we have found that the Framers of the Constitution used cryptography on a regular basis. Even the Constitution and the Bill of Rights themselves were often encoded as Thomas Jefferson and James Madison exchanged drafts of those documents. In fact, cryptography was used by a virtual who's who of the Framers of our Constitution, not only Jefferson and Madison, but Benjamin Franklin, Alexander Hamilton, John and Abigail Adams, Aaron Burr, and many others.

In sharp contrast to the administration's arguments today, they viewed cryptography as an essential instrument in protecting information, both political and personal. Our research indicates that when the first and fourth and fifth amendments were enacted in the late 1700's, any suggestion that the Government should have the ability to prevent individuals from encrypting their messages or that the Government should have a back-door key to all

encrypted messages would have struck the Constitution's Framers as ridiculous.

In sum, our legal challenge to the current restrictions on encryption software is succeeding. It is succeeding because the first amendment is clearly violated when the Government institutes a pre-publication licensing scheme that allows agency bureaucrats unfettered discretion to deny Americans the ability to publish their own ideas. It is succeeding because the courts have recognized the importance of keeping the first amendment intact as we move on to the information age. As you consider the many legislative proposals about cryptography, we hope that you will do the same.

Thank you.

Senator ASHCROFT. Thank you very much, Ms. Cohn.

[The prepared statement of Ms. Cohn follows:]

PREPARED STATEMENT OF CINDY A. COHN

I want to thank the Sub-Committee for inviting me here today. Although there have been very many hearings and much discussion about cryptography here in Washington, this is the first, I believe, to seek testimony from one of the attorneys directly involved in the legal challenges to the cryptography regulations.

I've been asked here because I am lead counsel in the case of *Bernstein* v. *Department of Justice, et al.* With the help of the Electronic Frontier Foundation, Professor Daniel J. Bernstein has been trying for over six years to publish on the Internet a simple cryptographic computer program which he wrote. He has been told that if he does, he will be prosecuted.

We argued that American scientists, be they academics, in industry or hobbyists, should not have to submit their own work prior to publication to faceless government bureaucrats. This is especially so when those same bureaucrats have unchecked discretion to bar them from publishing his work. That is what the current scheme allows. In fact, before we brought suit those same agency bureaucrats told Professor Bernstein that publishing an academic paper about his software would be illegal and that putting his software into a public library would be illegal. The Federal District Court for the Northern District of California has agreed with us that the regulations are in violation of the First Amendment on their face, meaning that they violate the First Amendment rights of all Americans, not just Professor Bernstein.

KARN AND JUNGER: TWO OTHER LEGAL CHALLENGES

Two other similar cases are also pending. The first *Karn* v. *U.S. Department of State,* is here in D.C. District Court. The *Karn* case is the clearest example of the quip often made about the Administration's cryptography policy—that it is based upon the belief that terrorists can't type. Mr. Karn was told that, although a book containing computer source code could be freely sent abroad, a floppy disk containing the exact same information could not. The second case *Junger* v. *Christopher,* is in Cleveland, Ohio, and is based upon the government's position that Professor Junger, a Law professor at Case Western University could be prosecuted for teaching a Computers and the Law course in his usual way.

RULINGS OF THE BERNSTEIN CASE

In the *Bernstein* case we have received three rulings from the District Court so far, all in our favor:

(1) April 1996: Computer program source code is speech;

(2) December 1996: ITAR was unconstitutional;

(3) August 1997: New Commerce Department cryptography regulations issued in December, 1996 are unconstitutional.

In short, the Federal District Court has declared that every single one of the current (and previous) regulations of encryption software are unconstitutional.

The final ruling in our favor was appealed by the Administration, argued in December, 1997 before the Ninth Circuit Court of Appeals, and is now awaiting decision. I have attached a copy of the third District Court opinion to my written statement for your review. I hope you have your staff take the time to review it—it gives a clear and concise statement of some of the key constitutional requirements that

any legislation on cryptographic software must meet and a better explanation than I could ever give you about why the current regulations are unconstitutional.

As I mentioned before, the *Bernstein* case challenges the current government restrictions on cryptographic software on the grounds that they are in violation of the First Amendment. Although our case focuses, as it must, on the current regulations, the analysis would apply as well to proposed domestic reatrictions which would restrict or license the creation, distribution or receipt of cryptographic software. Indeed the constitutional problems which would arise if domestic controls were imposed are even more severe than those of the current scheme.

The first doctrine of First Amendment law which the cryptography regulations violate is prior restraint of speech. The *Bernstein* case focuses on the easiest flaws to see in the current scheme—the lack of procedural protections. The Supreme Court has long held that if the government wants to institute a prepublication licensing scheme, it must contain:

(1) Prompt decision—no more than 2 weeks;

(2) Only a court can stop publication; the government must bring a court case rather than act administratively;

(3) Government bears burden of proof in Court.

This comes from a seminal Supreme Court case called *Freedman* v. *Maryland.*

I should point out that as I would like to take credit for our legal analysis, we were not the first to see this problem. In fact, the first people to point out this problem in the regulations were in the Justice Department's Office of Legal Counsel in 1978. You see, the agencies have known for 20 years that thia scheme is unconstitutional. Their own lawyers told them so. That is why you never hear them mention the First Amendment in their presentations to you.

COMPUTER SOFTWARE IS PROTECTED EXPRESSION

The key point in our case, and in your consideration of any proposed legislation, is that source code is protected expression for purposes of the First Amendment. On this point, the administration largely agrees. Let me repeat that—the Administration has not denied that in regulating computer software it is also regulating the "expressive activities" of Americans. This conclusion, which is obvious to anyone who has ever written or read a computer program, is also consistent with what Congress has repeatedly acknowledged. Software is treated as identical to other forms of protected expression in both the Copyright Act and the Freedom of Information Act.

From a legal standpoint, the *Bernstein* case is not complex, nor does it break any dramatic new ground. It simply asks the courts to recognize that the First Amendment extends to science on the Internet, just as it does to science on paper and in the classroom. For it is this scientific freedom which has allowed us to even have an Internet, as well as the many other technologies which we enjoy today.

OTHER FIRST AMENDMENT TESTS WHICH CRYPTOGRAPHY REGULATIONS MUST MEET

Up to this point everything I've said isn't just my opinion. It's been decided by the Federal District Court. My legal team and I believe that there are other strong Constitutional reasons which prevent the regulation of cryptographic software. The District Court did not need to address these additional reasons, since it agreed with us that the first alone was sufficient to invalidate the regulations.

In addition to procedural protections, the Constitution requires that any regulation which institutes a licensing scheme, or any other form of prior restraint, pass the strictest of teats. Even a claim of national security or public safety must be carefully weighed against our fundamental rights, and must be supported with hard evidence of direct, immediate and irreparable harm, not just conjecture and a few frightening scenarios.

Further, aside from prior restraint, a scheme which targets speech on the subject of cryptography and treats that speech differently from speech on other topics must pass the tests of strict scrutiny—that the regulation address a compelling government interest and be narrowly tailored to reach only that interest and no further. That is, the government's concern about national security cannot reach so broadly as to prevent law-abiding citizens from having access to software which they can use for completely lawful purposes. Put into another context, it means that the government cannot require all of us to deposit our house keya with them on the off chance that one of us is a criminal.

Further, the government must prove that their reatrictions on speech actually meet their goals. Here, such proof would be difficult since terrorists, pedophiles and drug dealers can simply purchase or download strong German, Swiss or Japanese encryption software that is freely available all over the U.S. and the world—over

500 at last count. If necessary, criminals could even type in or scan one of the computer programs printed in the many books published on the subject.

THE ADMINISTRATION'S LEGISLATIVE PROPOSALS FAIL THESE FIRST AMENDMENT TESTS

Neither the current scheme nor any administration-supported, so-called "compromise" schemes proposed so far addresses these First Amendment problems. And even the SAFE bill, which is well-intentioned, fails to contain an assurance of judicial review of any agency decision to prevent publication due to alleged national security concerns, a key element required by the Constitution. SAFE also does not clearly protect scientists such as Professor Bernstein, but only protects those who seek to distribute mass market software already available abroad. This means that American scientists can no longer participate in the ongoing international development of this vital and important area of science.

ENCRYPTED SPEECH IS STILL SPEECH

In addition, we believe that regulation of encryption software and technology violates the First Amendment because of what encryption does. Encryption allows people to use electronic envelopes to protect their speech. The Supreme Court has noted that a state could not regulate ink or paper without raising constitutional concerns. We believe that similarly the government cannot prevent Americans from using electronic envelopes or require them to use key-escrowed envelopes without violating their First Amendment rights. This is because such rules compel them to speak to the Government anytime they wish to speak to anyone else. Encrypted speech is still speech. The elimination of privacy creates a chilling effect on that speech which implicates the First Amendment.

ENCRYPTION WAS USED BY THE FOUNDING FATHERS

In fact, in our research for this case we have discovered that the Founding Fathers used cryptography on a regular basis. Even the Constitution and the Bill of Rights themselves were often encoded, as Thomas Jefferson and James Madison exchanged drafts of those seminal documents. Cryptography was used by a virtual Who's Who of the American Founding Fathers—not only Jefferson and Madison but Benjamin Franklin, Alexander Hamilton, John and Abigail Adams, Aaron Burr, and many others. In sharp contrast to the Administration's arguments today, they viewed cryptography as an essential instrument for protecting information, both political and personal. Our research indicates that when the First and Fourth Amendments were enacted in the late 1700s, any suggestion that the Government should have the ability to prevent individuals from encrypting their messages, or that the Government should have a back-door key to all encrypted messages, would have struck the Constitution's framers as ridiculous.

CONCLUSION

In sum, our legal challenge to the current restrictions on encryption software is succeeding. It is succeeding because the First Amendment is clearly violated when the government institutes a prepublication licensing scheme which allows agency bureaucrats unfettered discretion to prevent American scientists from publishing their own ideas. It is succeeding because the Courts have recognized the importance of keeping the First Amendment intact as we move into the information age. As you consider the many legislative proposals about cryptography, we hope you will do the same.

974 F.Supp. 1288
97 Daily Journal D.A.R. 13,899
(Cite as: 974 F.Supp. 1288)

Daniel J. BERNSTEIN, Plaintiff,
v.
UNITED STATES DEPARTMENT OF STATE, et al., Defendants.

No. C-95-0582 MHP.

United States District Court, N.D. California.

Aug. 25, 1997.

Mathematician sought declaratory and injunctive relief against enforcement of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) on the ground that they were unconstitutional on their face and as applied to the mathematician's cryptographic computer source code. On cross-motions for summary judgment, the District Court, 945 F.Supp. 1279, invalidated parts of the regulations. Mathematician filed an amended complaint after a new executive order transferred regulatory authority to the Department of Commerce. On various motions, the District Court, Patel, J., held that: (1) there was no basis for a statutory, non-constitutional challenge to the executive order; (2) the encryption regulations issued by the Bureau of Export Administration (BXA) were directed quite specifically and "by their terms" to the entire field of applied scientific research and discourse and, thus, were subject to a facial prior restraint analysis, even though the export of commercial cryptographic software programs may not have been undertaken for expressive reasons; and (3) the regulations were unconstitutional prior restraints in violation of the First Amendment, inasmuch as encryption software was singled out and treated differently from other software regulated under the Export Administration Regulations (EAR).

Ordered accordingly.

[1] CONSTITUTIONAL LAW ⇐ 46(1)
92k46(1)
Claim that President and Department of Commerce lacked statutory authority under International Emergency Economic Powers Act (IEEPA) to regulate computer software encryption products implicated validity of existing regulations and was to be addressed before review of any constitutional questions. International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706.

[2] WAR AND NATIONAL EMERGENCY ⇐ 504
402k504
President was not "agency" within meaning of Administrative Procedure Act (APA) and, thus, his actions in banning export of computer software encryption products under International Emergency Economic Powers Act (IEEPA) was not reviewable under APA. 5 U.S.C.A. § 551 et seq.; International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706.

See publication Words and Phrases for other judicial constructions and definitions.

[3] WAR AND NATIONAL EMERGENCY ⇐ 503
402k503
District court could not review non-Administrative Procedure Act (APA) statutory claims about whether President exceeded his statutory authority under International Emergency Economic Powers Act (IEEPA) to transfer jurisdiction over computer software encryption items to Commerce Department. 5 U.S.C.A. § 551 et seq.; International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706.

[4] WAR AND NATIONAL EMERGENCY ⇐ 504
402k504
Declaration of national emergency and issuance of executive order that transferred to Department of Commerce jurisdiction over export of nonmilitary computer software encryption products was action that rested with President and was based on his broad discretion under International Emergency Economic Powers Act (IEEPA); thus, legitimacy of executive order would not be addressed by district court. International

Emergency Economic Powers Act, §§ 202-207, 202, 50 U.S.C.A. §§ 1701-1706, 1701; Export Administration Act of 1979, § 2 et seq., 50 App.U.S.C.A. § 2401 et seq.; 15 C.F.R. § 730.1 et seq.

[5] WAR AND NATIONAL EMERGENCY ⇐ 501
402k501
Computer encryption software was "property in which any foreign country or a national thereof has any interest," within meaning of International Emergency Economic Powers Act (IEEPA) and, thus, encryption software was subject to regulation, despite mathematician's claim that, as speech, encryption software was within exemption for personal communications and informational materials. International Emergency Economic Powers Act, §§ 202-207, 203(a)(1), (b)(1, 3), 50 U.S.C.A. §§ 1701-1706, 1702(a)(1), (b)(1, 3); 31 C.F.R. §§ 500.311, 500.312.

See publication Words and Phrases for other judicial constructions and definitions.

[6] WAR AND NATIONAL EMERGENCY ⇐ 504
402k504
Cryptographic computer software was not "any postal, telegraphic, telephonic or other personal communication which does not transfer anything of value" within meaning of exemption from regulation under International Emergency Economic Powers Act (IEEPA); encryption software was not limited to academic discussion of cryptographic ideas, and there were potentially billions of dollars at stake in export of commercial encryption software. U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 203(a)(1), (b)(1, 3), 50 U.S.C.A. §§ 1701-1706, 1702(a)(1), (b)(1, 3); 31 C.F.R. §§ 500.311, 500.312.

See publication Words and Phrases for other judicial constructions and definitions.

[7] WAR AND NATIONAL EMERGENCY ⇐ 504
402k504
Computer software encryption products were within scope of Export Administration Act (EAA) as items controlled for foreign policy or national security reasons and, thus, those products did not fall within exemption from International Emergency Economic Powers Act (IEEPA) for informational materials. U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 203(b)(3), 50 U.S.C.A. §§ 1701-1706, 1702(b)(3); Export Administration Act of 1979, §§ 2 et seq., 5(a)(1), 6(a)(1), 50 App.U.S.C.A. §§ 2401 et seq., 2404(a)(1), 2405(a)(1).

[8] CONSTITUTIONAL LAW ⇐ 90.1(1)
92k90.1(1)
Narrow determination that source code for computer software encryption products was "speech" protected by First Amendment did not remove encryption technology from all government regulation under International Emergency Economic Powers Act (IEEPA). U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 203(a)(1), (b)(1, 3), 50 U.S.C.A. §§ 1701-1706, 1702(a)(1), (b)(1, 3); 31 C.F.R. §§ 500.311, 500.312.

See publication Words and Phrases for other judicial constructions and definitions.

[8] WAR AND NATIONAL EMERGENCY ⇐ 501
402k501
Narrow determination that source code for computer software encryption products was "speech" protected by First Amendment did not remove encryption technology from all government regulation under International Emergency Economic Powers Act (IEEPA). U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 203(a)(1), (b)(1, 3), 50 U.S.C.A. §§ 1701-1706, 1702(a)(1), (b)(1, 3); 31 C.F.R. §§ 500.311, 500.312.

See publication Words and Phrases for other judicial constructions and definitions.

[9] CONSTITUTIONAL LAW ⇐ 90(3)
92k90(3)

Chief purpose of constitutional protection afforded by First Amendment is to prevent prior restraints on publication. U.S.C.A. Const.Amend. 1.

[10] CONSTITUTIONAL LAW ⇐ 90(3)
92k90(3)
Governments may impose valid time, place and manner restrictions when they are content-neutral, narrowly tailored to serve substantial governmental interest, and leave open alternative channels for communication, but government may not condition speech on obtaining license or permit from government official in that official's boundless discretion. U.S.C.A. Const.Amend. 1.

[10] CONSTITUTIONAL LAW ⇐ 90.1(4)
92k90.1(4)
Governments may impose valid time, place and manner restrictions when they are content-neutral, narrowly tailored to serve substantial governmental interest, and leave open alternative channels for communication, but government may not condition speech on obtaining license or permit from government official in that official's boundless discretion. U.S.C.A. Const.Amend. 1.

[11] CONSTITUTIONAL LAW ⇐ 90.1(1)
92k90.1(1)
First Amendment is more tolerant of subsequent criminal punishment of speech than it is of prior restraints on same speech. U.S.C.A. Const.Amend. 1.

[12] CONSTITUTIONAL LAW ⇐ 90(3)
92k90(3)
Danger inherent in prior restraint is largely procedural, in that restraint bypasses judicial process and locates in government official the delicate responsibility of passing on permissibility of speech. U.S.C.A. Const.Amend. 1.

[13] CONSTITUTIONAL LAW ⇐ 90.1(4)
92k90.1(4)
When risks of prior restraint associated with unbridled licensing schemes are present to significant degree, courts must entertain immediate facial attack on law. U.S.C.A. Const.Amend. 1.

[14] CONSTITUTIONAL LAW ⇐ 90.1(1)
92k90.1(1)
Computer software encryption regulations issued by Bureau of Export Administration (BXA) were directed quite specifically and "by their terms" to entire field of applied scientific research and discourse and, thus, were subject to facial prior restraint analysis, even though export of commercial cryptographic software program may not have been undertaken for expressive reasons; activity is often undertaken by scientists for purely expressive reasons. U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706; Export Administration Act of 1979, § 2 et seq., 50 App.U.S.C.A. § 2401 et seq.; 15 C.F.R. § 730.1 et seq.

[15] CONSTITUTIONAL LAW ⇐ 90.1(1)
92k90.1(1)
Computer encryption regulations issued by Bureau of Export Administration (BXA) were unconstitutional prior restraints in violation of First Amendment; encryption software was singled out and treated differently from other software regulated under Export Administration Regulations (EAR), although exception existed for printed materials, exception was unreliable because BXA reserved right to control scannable source code in printed form, exception sought to codify distinction between paper and electronic publication that made little or no sense and was untenable, and Internet was subject to same exacting level of First Amendment scrutiny as print media. U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706; Export Administration Act of 1979, § 2 et seq., 50 App.U.S.C.A. § 2401 et seq.; 15 C.F.R. § 730.1 et seq.

[15] CONSTITUTIONAL LAW ⇐ 90.1(9)
92k90.1(9)
Computer encryption regulations issued by Bureau of Export Administration (BXA) were unconstitutional prior restraints in violation of First Amendment; encryption software was singled out and treated differently from other software regulated under Export Administration Regulations (EAR), although

exception existed for printed materials, exception was unreliable because BXA reserved right to control scannable source code in printed form, exception sought to codify distinction between paper and electronic publication that made little or no sense and was untenable, and Internet was subject to same exacting level of First Amendment scrutiny as print media. U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706; Export Administration Act of 1979, § 2 et seq., 50 App.U.S.C.A. § 2401 et seq.; 15 C.F.R. § 730.1 et seq.

[15] WAR AND NATIONAL EMERGENCY ⇐ 504
402k504
Computer encryption regulations issued by Bureau of Export Administration (BXA) ware unconstitutional prior restraints in violation of First Amendment; encryption software was singled out and treated differently from other software regulated under Export Administration Regulations (EAR), although exception existed for printed materials, exception was unreliable because BXA reserved right to control scannable source code in printed form, exception sought to codify distinction between paper and electronic publication that made little or no sense and was untenable, and Internet was subject to same exacting level of First Amendment scrutiny as print media. U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706; Export Administration Act of 1979, § 2 et seq., 50 App.U.S.C.A. § 2401 et seq.; 15 C.F.R. § 730.1 et seq.

[16] CONSTITUTIONAL LAW ⇐ 90.1(1)
92k90.1(1)
Computer encryption regulations issued by Bureau of Export Administration (BXA) did not need to regulate software directly for its content in order to make regulations function as unconstitutional prior restraint on speech; it would be enough that they were directed at expressive activity. U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706; Export Administration Act of 1979, § 2 et seq., 50 App.U.S.C.A. § 2401 et seq.; 15 C.F.R. § 730.1 et seq.

[16] WAR AND NATIONAL EMERGENCY ⇐ 504
402k504
Computer encryption regulations issued by Bureau of Export Administration (BXA) did not need to regulate software directly for its content in order to make regulations function as unconstitutional prior restraint on speech; it would be enough that they were directed at expressive activity. U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706; Export Administration Act of 1979, § 2 et seq., 50 App.U.S.C.A. § 2401 et seq.; 15 C.F.R. § 730.1 et seq.

[17] CONSTITUTIONAL LAW ⇐ 90.1(4)
92k90.1(4)
Computer software encryption regulations issued by Bureau of Export Administration (BXA) pursuant to Export Administration Regulations (EAR) did not have sufficient procedural safeguards to withstand prior restraint challenge; although regulations provided that license applications would be resolved or referred to President within 90 days, there was no time limit on application referred to President, internal appeals process required only that agency "shall decide an appeal within a reasonable time after receipt of the appeal," no standards existed for ruling on applications, and internal appellate decision was final and not subject to judicial review. U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706; Export Administration Act of 1979, §§ 2 et seq., 13(e), 50 App.U.S.C.A. §§ 2401 et seq., 2412(e); 15 C.F.R. §§ 730.1 et seq., 750.4(a), 756.2(c)(1, 2).

[17] WAR AND NATIONAL EMERGENCY ⇐ 504
402k504
Computer software encryption regulations issued by Bureau of Export Administration (BXA) pursuant to Export Administration Regulations (EAR) did not have sufficient procedural safeguards to withstand prior

restraint challenge; although regulations provided that license applications would be resolved or referred to President within 90 days, there was no time limit on application referred to President, internal appeals process required only that agency "shall decide an appeal within a reasonable time after receipt of the appeal," no standards existed for ruling on applications, and internal appellate decision was final and not subject to judicial review. U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706; Export Administration Act of 1979, §§ 2 et seq., 13(e), 50 App.U.S.C.A. §§ 2401 et seq., 2412(e); 15 C.F.R. §§ 730.1 et seq., 750.4(a), 756.2(c)(1, 2).

[18] CONSTITUTIONAL LAW ⇐ 47
92k47
First Amendment does not render inapplicable the rule that federal court should not extend its invalidation of statute further than is necessary to dispose of case before court. U.S.C.A. Const.Amend. 1.

[19] DECLARATORY JUDGMENT ⇐ 304
118Ak304
Departments of Energy (DOE) and Justice (DOJ) and Central Intelligence Agency (CIA) were not appropriate defendants in action challenging regulations that restricted exportation of encryption software, even though officials from each agency were involved in some way with licensing reviews; roles played by DOE, DOJ and CIA are limited to consulting and advising Secretary of Commerce who was responsible for final decisions on export licenses. U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706; Export Administration Act of 1979, § 2 et seq., 50 App.U.S.C.A. § 2401 et seq.; 15 C.F.R. §§ 730.1 et seq., 750.4(d, e), 772.

[20] CIVIL RIGHTS ⇐ 262.1
78k262.1
Mathematician who challenged enforcement of Arms Export Control Act (AECA) and International Traffic in Arms Regulations (ITAR) on prior restraint grounds was entitled to injunction against enforcement of regulations against him or against anyone who sought to use, discuss or publish his encryption program, in order to protect mathematician from fear of prosecution for teaching and writing about encryption. U.S.C.A. Const.Amend. 1; International Emergency Economic Powers Act, §§ 202-207, 50 U.S.C.A. §§ 1701-1706; Export Administration Act of 1979, § 2 et seq., 50 App.U.S.C.A. § 2401 et seq.; 15 C.F.R. § 730.1 et seq.

*1291 Cindy A. Cohn, McGlashan & Sarrail, San Mateo, CA, Lee Tien, Berkeley, CA, M. Edward Ross, Steefel, Levitt & Weiss, San Francisco, CA, James R. Wheaton, Environmental Law Foundation, Oakland, CA, for Plaintiff.

Frank W. Hunger, Asst. Atty. Gen., U.S. Dept. of Justice Torts, Civil Div., San Francisco, CA, Michael J. Yamaguchi, U.S. Atty., Mary Beth Uitti, U.S. Attorney's Office, San Francisco, CA, Vincent M. Garvey, U.S.D.J.-Civil Div., Washington, DC, Anthony J. Coppolino, U.S. Dept. of Justice, Civil Division-Federal Programs Branch, Washington, DC, for Defendants.

OPINION

PATEL, District Judge.

Plaintiff Daniel Bernstein originally brought this action against the Department of State and the individually named defendants seeking declaratory and injunctive relief from their enforcement of the Arms Export Control Act ("AECA"), 22 U.S.C. § 2778 (1990), and the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. Pts. 120-30 (1994), on the grounds that they are unconstitutional on their face and as applied to plaintiff. The court granted in part and denied in part the parties' cross motions for summary judgment on December 9, 1996. Just prior to the court's order, President Clinton by Executive Order 13026 transferred jurisdiction over the export of nonmilitary encryption products to the Department of Commerce pursuant to the Export Administration Act of 1979 ("EAA"),

50 U.S.C.App. §§ 2401 et seq. (1991), and the Export Administration Regulations ("EAR"), 15 C.F.R. Pt. 730 et seq. (1997). On December 30, 1996, the Commerce Department issued an interim rule regulating the export of certain *1292 encryption products. 61 Fed.Reg. 68572 (Dec. 30, 1996). Plaintiff subsequently amended his complaint to include the new regulations and new defendants. Now before this court are the parties' second cross-motions for summary judgment on the question of whether the licensing requirements for the export of cryptographic devices, software and related technology covered by the amendments to the EAR constitute an impermissible infringement on speech in violation of the First Amendment.

Having considered the parties' arguments and submissions, and for the reason set forth below, the court enters the following memorandum and order.

BACKGROUND [FN1]

FN1. Some of the information in this section is taken directly from the court's previous opinions in this action, Bernstein v. United States Dept. of State, 922 F.Supp. 1426 (N.D.Cal.1996) (Bernstein I), and Bernstein v. United State Dept. of State, 945 F.Supp. 1279 (N.D.Cal.1996) (Bernstein II); other background information is left out or condensed and reference is made to those opinions. Additional information comes from the parties' current submissions or other sources as indicated.

At the time this action was filed, plaintiff was a PhD candidate in mathematics at University of California at Berkeley working in the field of cryptography, an area of applied mathematics that seeks to develop confidentiality in electronic communication. Plaintiff is currently a Research Assistant Professor in the Department of Mathematics, Statistics and Computer Science at the Encryption basically involves running a readable message known as University of Illinois at Chicago.

I. Cryptography

Encryption basically involves running a readable message known as "plaintext" through a computer program that translates the message according to an equation or algorithm into unreadable "ciphertext." Decryption is the translation back to plaintext when the message is received by someone with an appropriate "key." The message is both encrypted and decrypted by compatible keys. [FN2] The uses of cryptography are far-ranging in an electronic age, from protecting personal messages over the Internet and transactions on bank ATMs to ensuring the secrecy of military intelligence. In a prepublication copy of a report done by the National Research Council ("NRC") at the request of the Defense Department on national cryptography policy, the NRC identified four major uses of cryptography: ensuring data integrity, authenticating users, facilitating nonrepudiation (the linking of a specific message with a specific sender) and maintaining confidentiality. Tien Decl., Exh. E, National Research Council, National Academy of Sciences, Cryptograph's Role in Securing the Information Society C-2 (Prepublication Copy May 30, 1996) (hereinafter "NRC Report").

FN2. In symmetric cryptography the encryption key is the same as the decryption key. Asymmetric, or public-key, cryptography uses different keys for encryption and decryption and generally only the encryption key is disclosed.

Once a field dominated almost exclusively by governments concerned with protecting their own secrets as well as accessing information held by others, the last twenty years has seen the popularization of cryptography as industries and individuals alike have increased their use of electronic media and have sought to protect their electronic products and communications. NRC Report at vii. As part of this transformation, cryptography has also become a dynamic academic discipline within applied mathematics. Appel Dec. at 5; Blaze Dec. at 2.

II. Prior Regulatory Framework

Plaintiff's original complaint and both of the court's decisions in this action were directed at the regulations in force at the time, the ITAR, promulgated to implement the AECA. The ITAR, administered within the State Department by the Director of the Office of Defense Trade Controls ("ODTC"), Bureau of Politico-Military Affairs, regulates the import and export of defense articles and defense services by designating such items to the United States Munitions List ("USML"). 22 U.S.C. § 2778(a)(1). [FN3] Items listed on the USML, which at the time included all cryptographic systems and software, require a license before they can be *1293 imported or exported. 22 U.S.C. § 2778(b)(2). The ITAR allows for a "commodity jurisdiction procedure" by which the ODTC determines if an article or service is covered by the USML when doubt exists about an item. 22 C.F.R. § 120.4(a).

FN3. For a full description of the ITAR, see Bernstein I, 922 F.Supp. at 1429-30 and Bernstein II, 945 F.Supp. at 1283-84.

As a graduate student, Bernstein developed an encryption algorithm he calls "Snuffle." He describes Snuffle as a zero-delay private-key encryption system. Complaint Exh. A. Bernstein has articulated his mathematical ideas in two ways: in an academic paper in English entitled "The Snuffle Encryption System," and in "source code" written in "C", a high-level computer programming language, [FN4] detailing both the encryption and decryption, which he calls "Snuffle.c" and "Unsnuffle.c", respectively. Once source code is converted into "object code," a binary system consisting of 0s and 1s read by a computer, the computer is capable of encrypting and decrypting data.

FN4. Source code is the text of a source program and is generally written in a high-level language that is two or more steps removed from machine language which is a low-level language. High-level languages are closer to natural language than low-level languages which direct the functioning of the computer. Source code must be translated by way of a translating program into machine language before it can be read by a computer. The object code is the output of that translation. It is possible to write a source program in high-level language without knowing about the actual functions of the computer that carry out the program. Encyclopedia of Computer Science 962, 1263-64 (Anthony Ralston & Edwin D. Reilly eds., 3d ed. 19 § 5)

In 1992 plaintiff submitted a commodity jurisdiction ("CJ") request to the State Department to determine whether Snuffle.c and Unsnuffle.c (together referred to as Snuffle 5.0), each submitted in C language source files, and his academic paper describing the Snuffle system, were controlled by ITAR. [FN5] The ODTC determined that the commodity Snuffle 5.0 was a defense article on the USML under Category XIII of the ITAR and subject to licensing by the Department of State prior to export. The ODTC identified the item as a "stand-alone cryptographic algorithm which is not incorporated into a finished software product." Complaint Exh. B.

FN5. Again, a more detailed description of plaintiff's communications with the ODTC appears in Bernstein I, 922 F.Supp. at 1430, and Bernstein II, 945 F.Supp. at 1284-85. Those opinions also describe the confusion surrounding the determination of the academic paper.

Alleging that he was not free to teach, publish or discuss with other scientists his theories on cryptography embodied in his Snuffle program, plaintiff brought this action challenging the AECA and the ITAR on the grounds that they violated the First Amendment. In Bernstein I this court found that source code was speech for purposes of the First Amendment and therefore plaintiff's claims presented a colorable constitutional challenge and were accordingly justiciable. In Bernstein II the court concluded that the licensing requirements for encryption software under the ITAR constituted an unlawful prior restraint. The court also considered vagueness

and overbreadth challenges to certain terms contained in the ITAR. The court issued its decision in Bernstein II on December 9, 1996.

III. The Transfer of Jurisdiction and the Current Regulatory Framework

On November 15, 1996, President Clinton issued Executive Order 13026, titled "Administration of Export Controls on Encryption Products," in which he ordered that jurisdiction over export controls on nonmilitary encryption products and related technology be transferred from the Department of State to the Department of Commerce. The President's Executive Order specifies that encryption products that would be designated as defense articles under the USML and regulated under the AECA are now to be placed on the Commerce Control List ("CCL") under the EAR. The White House Press Release accompanying the Executive Order clarified that encryption products designed for military applications would remain on the USML and continue to be regulated under the ITAR. Press Release Accompanying Exec. Order No. 13026, at 2 (hereinafter "Press Release"). The Executive Order also provides a caveat that is repeated in the Press Release and throughout the new regulations: "the export of encryption software, like the export of other encryption products described in this section, must be controlled because of such software's functional capacity, *1294 rather than because of any possible informational value of such software...." Exec. Order No. 13026, 61 Fed.Reg. 58768 (1996). The Press Release states that encryption products must be controlled for foreign policy and national security interests and concludes by noting that if the new regulations do not provide adequate controls on encryption products then such products will be redesignated as defense articles and placed again on the USML. Press Release, at 1, 4.

The EAR were promulgated to implement the EAA, but the EAA is not permanent legislation. Lapses in the EAA have been declared national emergencies and the President has issued Executive Orders authorizing continuation of the EAR export controls under the authority of the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701-1706. See e.g., Exec. Order No. 12924, 59 Fed.Reg. 43437 (1994). Executive Order 13026 states that the authority of the President to administer these changes in the export control system under the EAR derives in part from the IEEPA and that the new controls on encryption products are "additional steps with respect to the national emergency described and declared" in the previous Executive Orders continuing in effect the EAR. Exec. Order No. 13026, 61 Fed.Reg. 58767 (1996).

On December 30, 1996, the Bureau of Export Administration ("BXA") under the Department of Commerce issued an interim rule amending the EAR "by exercising jurisdiction over, and imposing new combined national security and foreign policy controls on, certain encryption items that were on the [USML]." 61 Fed.Reg. 68572 (1996) (to be codified at 15 C.F.R. Pts. 730-774) ("encryption regulations" or "new regulations"). The EAR is structured around the CCL, 15 C.F.R. Pt. 774, 61 Fed.Reg. 12937 (1996), which categorizes items whose export is regulated according to various criteria, including the reason for their control. The new regulations add a category called "Encryption Items" or "EI" as a reason for control. 61 Fed.Reg. 68579 (1996) (to be codified at 15 C.F.R. § 738.2(d)(2)(i)(A)). Encryption items are defined as "all encryption commodities, software, and technology that contain encryption features and are subject to the EAR." 61 Fed.Reg. 68585 (to be codified at 15 C.F.R. § 772). This does not include those items still listed on the USML and controlled by the Department of State. With certain exceptions, one must obtain a license from the BXA prior to exporting any item listed on the CCL. See 15 C.F.R. Pts. 740-44. All items on the CCL are given an Export Control Classification Number ("ECCN") which can be used to determine the categories under which an item is controlled and the reasons for its control.

The new regulations add three categories of

items to the CCL which are controlled for EI reasons, [FN5] all of them more generally classified in Category 5, which covers telecommunications and information security. See 15 C.F.R. § 738.2(a). Those items are ECCN 5A002, covering encryption commodities; ECCN 5D002, covering encryption software; and ECCN 5E002, covering encryption technology. 61 Fed.Reg. 68586-87 (to be codified at 15 C.F.R. § 774 supp. D). For export licensing purposes, encryption software is treated the same as an encryption commodity. See note following ECCN 5D002. A commodity is defined generally as "[a]ny article, material, or supply except technology and software." 61 Fed.Reg. 68585 (to be codified at 15 C.F.R. Pt. 772). Encryption software is regulated differently from other software controlled by the CCL and is defined as "[c]omputer programs that provide capability of encryption functions or confidentiality of information or information systems. Such software includes source code, object code, applications software, or system software." 61 Fed.Reg. 68585 (to be codified at 15 C.F.R. Pt. 772). [FN7] Definitions of *1295 encryption source code and encryption object code have also been added. [FN8] Technology has not been amended by the encryption regulations and is defined generally as the technical data or technical assistance necessary for the development or use of a product. 15 C.F.R. Pt. 772. Controlled technology is that technology required for the development or use of items on the CCL. 15 C.F.R. Pt. 774 supp. 2 (General Technology Note). New restrictions on technical assistance have been added, however, to require a license to provide technical assistance (including training) to foreign persons with the intent to aid them in the foreign development of items that if they were domestic would be controlled under ECCNs 5A002 and 5D002. [FN9] 61 Fed.Reg. 68584 (to be codified at 15 C.F.R. § 744.9(a)); 61 Fed.Reg. 68579 (to be codified at 15 C.F.R. § 736.2(b)(7)(ii)).

FN6. These items are also controlled for national security and anti-terrorism reasons. 61 Fed.Reg. 68586-87 (to be codified at 15 C.F.R. § 774 supp. 1).

FN7. Under Part 772 of the new regulations which is dedicated to definitions of terms, the term "commodity" contains the following note: Note that the provisions of the EAR applicable to the control of software (e.g. publicly available provisions) are not applicable to encryption software. Encryption software is controlled because, like the items controlled under ECCN 5A002, it has a functional capacity to encrypt information on a computer system, and not because of any informational or theoretical value that such software may reflect, contain or represent, or that its export may convey to others abroad. 61 Fed.Reg. 68585 (to be codified at 15 C.F.R. Pt. 772).

FN8. Encryption source code is defined as "[a] precise set of operating instructions to a computer that, when compiled, allows for the execution of an encryption function on a computer." Encryption object code is defined as "[c]omputer programs containing an encryption source code that has been compiled into a form of code that can be directly executed by a computer to perform an encryption function." 61 Fed.Reg. 68585 (to be codified at 15 C.F.R. Pt. 772).

FN9. This provision notes "that the mere teaching or discussion of information about cryptography, including, for example, in an academic setting, by itself would not establish the intent described in this section, even where foreign persons are present." 61 Fed.Reg. 68584 (to be codified at 15 C.F.R. § 744.9(a)).

The EAR defines export as "an actual shipment or transmission of items subject to the EAR out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States...." 15 C.F.R. § 734.2(b)(1). The encryption regulations add a specific definition of export for encryption source code and object code software controlled under ECCN 5D002 which includes

downloading, or causing the downloading of,

such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the United States, over wire, cable, radio, electromagnetic, photooptical, photoelectric or other comparable communication facilities accessible to persons outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites, unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States.

61 Fed.Reg. 68578 (to be codified at 16 C.F.R. § 734.2(b)(9)).

A number of licensing exceptions are available under the EAR. See 15 C.F.R. Pt. 740. Under the encryption regulations, after a one-time review by BXA, licensing exceptions will be available for certain commercial encryption items, including mass-market encryption software, key-recovery software and commodities, and non-recovery encryption items up to 56-bit key length DES or equivalent strength software accompanied by a commitment to develop recoverable items. 61 Fed.Reg. 68581 (to be codified at 15 C.F.R. § 742.15). In general, items that are already publicly available or contain "de minimus" domestic content are not subject to the EAR. 15 C.F.R. §§ 734.3(b)(3) & 734.4. However, as directed by the President and implemented by the new regulations, these exceptions do not apply to encryption commodities or software. 61 Fed.Reg. 68577-78 (to be codified at 15 C.F.R. §§ 732.2(b) & (d), 734.3(b)(3), 734.4(b)); Exec. Order No. 13026, 61 Fed.Reg. 58768 (1996) ("I have determined that the export of encryption products described in this section could harm national security and foreign policy interests even where comparable products are or appear to be available from sources outside the United States ... "). This exception for encryption software to the general exclusion of publicly available items appears to pertain to publicly available or published information and software within the United States as well. 61 Fed.Reg. 68578 (to be codified at 15 C.F.R. § 734.7(c)). In addition, the EAR allows for broadly defined exceptions from the regulations for information resulting from fundamental research and educational information. 15 C.F.R. §§ 734.8, 734.9, & supp. 1. Neither *1296 of these exceptions applies to encryption software controlled under ECCN 5D002. 61 Fed.Reg. 68579 (to be codified at 15 C.F.R. §§ 734.8, 734.9). They do appear to apply to encryption technology. Finally, phonographic records and most printed matter are not subject to the EAR and encryption software is not exempted from this exclusion. 15 C.F.R. § 734.3(b)(2). Indeed, an intriguing if somewhat baffling note appears in the new regulations: "A printed book or other printed material setting forth encryption source code is not itself subject to the EAR (see § 734.3(b)(2)). "However, notwithstanding § 734.3(b)(2), encryption source code in electronic form or media (e.g. computer diskette or CD ROM) remains subject to the EAR (see § 734.3(b)(3))." [FN10] 61 Fed.Reg. 68578 (to be codified at 15 C.F.R. § 734.3).

FN10. The introductory information about the new regulations includes the following with respect to the exception for printed materials: "The administration continues to review whether and to what extent scannable encryption source or object code in printed form should be subject to the EAR and reserves the option to impose export controls on such software for national security and foreign policy reasons." 61 Fed.Reg. 68575.

Licenses are required for export of items controlled by ECCNs 5A002, 5D002 and 5E002 for all destinations except Canada. 61 Fed.Reg. 68580 (to be codified at 15 C.F.R. § 742.15(a)). Applications for licenses "will be reviewed on a case-by-case basis by BXA, in conjunction with other agencies, to determine whether the export or reexport is consistent with U.S. national security and foreign policy interests." 61 Fed.Reg. 68581 (to be codified at 15 C.F.R. § 742.15(b)). The EAR provides that license applications will be resolved or referred to the President within 90 days. 15 C.F.R. § 750.4(a). While an applicant who is denied a license is informed of appeal procedures, 15 C.F.R. § 750.6(a)(6), the EAR

does not appear to allow for judicial review. 15 C.F.R. § 756.2(c)(2); 50 U.S.C.App. § 2412(a).

LEGAL STANDARD

Under Federal Rule of Civil Procedure 56, summary judgment shall be granted "against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial ... since a complete failure of proof concerning an essential element of the nonmoving party's case necessarily renders all other facts immaterial." Celotex Corp. v. Catrett, 477 U.S. 317, 322-23, 106 S.Ct. 2548, 2552, 91 L.Ed.2d 265 (1986); see also T.W. Elec. Serv. v. Pacific Elec. Contractors Ass'n, 809 F.2d 626, 630 (9th Cir.1987) (the nonmoving party may not rely on the pleadings but must present significant probative evidence supporting the claim); Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248, 106 S.Ct. 2505, 2510, 91 L.Ed.2d 202 (1986) (a dispute about a material fact is genuine "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party.").

The court's function, however, is not to make credibility determinations, Anderson, 477 U.S. at 249, 106 S.Ct. at 2510-11, and the inferences to be drawn from the facts must be viewed in a light most favorable to the party opposing the motion. T.W. Elec. Serv., 809 F.2d at 631.

Where as here, the question is purely a legal one involving no disputes of material fact, the matter is appropriately handled on a motion for summary judgment.

DISCUSSION

Plaintiff contends that the EAR, specifically the amendments regulating encryption items, both facially and as applied, constitutes a prior restraint on plaintiff's right to free speech, is unconstitutionally vague and overbroad, is content-based, and violates his freedom of association. Plaintiff also claims that the presidential transfer of jurisdiction to the Commerce Department and the encryption regulations themselves exceed their statutory authority and are ultra vires. Plaintiff requests declaratory and nationwide injunctive relief. In addition to opposing plaintiff's claims, defendants seek to dismiss certain defendants as extraneous and ask that the court vacate its decision in Bernstein II.

I. Statutory Authority of the President and the Agency to Regulate Encryption Items

[1] In his amended complaint plaintiff alleges that the presidential transfer of jurisdiction *1297 and the subsequent agency regulations are ultra vires because the President and the Department of Commerce lacked statutory authority under the IEEPA to regulate encryption products. Plaintiff contends that the IEEPA, by its own terms, restricts the regulation of information protected by the First Amendment. Plaintiff also argues that use of the IEEPA requires an international emergency, which is not identified in the President's Executive Order. Plaintiff also maintains that the regulation of encryption products by the President and the Secretary violates the APA.

Defendants contend that the court lacks jurisdiction to review presidential determinations under the IEEPA. To the extent a claim may still lie against the Secretary, defendants argue that the IEEPA does not preclude export controls on encryption items.

Although the parties do not identify this claim as a threshold issue, plaintiff's argument is that the transfer of jurisdiction to Commerce and the Secretary's regulations were in excess of their statutory authority and are therefore invalid. To the extent this issue implicates the very validity of the current regulations, the court finds that it should be addressed before a review on the merits. In addition, courts must consider nonconstitutional questions before reaching constitutional considerations in order to avoid passing on constitutionality where possible. Jean v. Nelson, 472 U.S. 846, 854, 105 S.Ct.

2992, 2996-97, 86 L.Ed.2d 664 (1985).

A. The IEEPA

The IEEPA authorizes the President "to deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat." 50 U.S.C. § 1701(a). Under this authority the President may "investigate, regulate, or prohibit any transaction in foreign exchange," 50 U.S.C. § 1702(a)(1)(A)(i), and "investigate, regulate, direct and compel, nullify, void, prevent or prohibit, any ... exportation of ... any property in which any foreign country or a foreign national thereof has any interest...." 50 U.S.C. § 1702(a)(1)(B). However, the IEEPA axplicitly excludes any authority

> to regulate or prohibit, directly or indirectly--any postal, telegraphic, or other personal communication, which does not involve a transfer of anything of value; ... or the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.

50 U.S.C. § 1702(b)(1) & (3) (1991 & Supp.1996). The statute goes on to limit the above exemption to those exports which ere not otherwise controlled under sections 2404 and 2405 of the EAA. 50 U.S.C. § 1702(b)(3).

The IEEPA was passed in 1977 as a refinement of the Trading With the Enemy Act of 1917 ("TWEA"), which at the time provided a source of presidential emergency authority. S.Rep. No. 95-466, at 2 (1977), reprinted in 1977 U.S.C.C.A.N. 4540,4541. In the Senate Report accompanying the passage of the IEEPA, the Committee suggests that what became section 1702(b) was intended to exclude donations and humanitarian contributions from emergency regulation so long as such transfers did not subvert the effective exercise of emergency authority. S.Rep. No. 95-466, at 5 Section 1702(b)(3) of the IEEPA was enacted in 1988 and amended in 1994 to broaden and strengthen the exemption for informational materials. According to the House Conference Report, language adopted in 1988 was intended to ensure "that no embargo may prohibit or restrict directly or indirectly the import or export of information that is protected under the First Amendment to the U.S. Constitution. The language was explicitly intended, by including the words 'directly or indirectly' to have a broad scope." H.R. Con. Rep. No. 103-482, at 239 (1994), reprinted in 1994 U.S.C.C.A.N. 302, 483. However, overly-narrow interpretations of section 1702(b)(3) by the Treasury Department prompted the 1994 amendment to "facilitate transactions and activities incident to *1298 the flow of information and informational materials without regard to the type of information, its format, or means of transmission, and electronically transmitted information...." H.R. Con. Rep. No. 103-482, at 239.

B. Statutory Authority of the President to Regulate Encryption Items Under the IEEPA

[2] Plaintiff argues that President Clinton exceeded his authority under the IEEPA because the encryption items regulated are properly exempt from regulation under section 1702(b) and because the transfer was not a temporary exercise of emergency authority. [FN11] Defendants claim that the President's actions are not reviewable.

> FN11. At oral argument plaintiff retreated from his position that the ultra vires claim was directed at the President. However, Count VI of plaintiff's supplemental complaint clearly alleges that the President's actions exceeded his authority under the IEEPA.

It is clear that the President's order is not reviewable under the APA. Franklin v. Massachusetts, 505 U.S. 788, 796, 112 S.Ct. 2767, 2773, 120 L.Ed.2d 636 (1992). In

Franklin, an action seeking APA review of the decennial reapportionment of the House of Representatives, the Supreme Court concluded that "the final action complained of is that of the President, and the President is not an agency within the meaning of the [APA]." Id. The Court went on to note that the President's actions were still reviewable for constitutionality. Id. at 801, 112 S.Ct. at 2775-76.

[3] Less clear is the extent to which a court may review a non-APA claim that the President exceeded his statutory authority where there is no allegation of a constitutional violation. Not long after Franklin the Supreme Court decided Dalton v. Specter, 511 U.S. 462, 114 S.Ct. 1719, 128 L.Ed.2d 497 (1994), in which it reviewed a claim that the President exceeded his statutory authority under the Defense Base Closure and Realignment Act. The court below had attempted to follow Franklin by reasoning that when the President's actions exceed his statutory authority he also violates the constitutional separation of powers doctrine. Id. at 471, 114 S.Ct. at 1725. The Dalton Court rejected this conclusion, holding that "claims simply alleging that the President has exceeded his statutory authority are not 'constitutional' claims, subject to judicial review under the exception recognized in Franklin." Id. at 473-74, 114 S.Ct. at 1726-27 (footnote omitted). However, the Court did not rule out the possibility of judicial review of statutory claims entirely.

> We may assume for the sake of argument that some claims that the President has violated a statutory mandate are judicially reviewable outside the framework of the APA. But longstanding authority holds that such review is not available when the statute in question commits the decision to the discretion of the President.

Id. at 474, 114 S.Ct. at 1727 (citing Dames & Moore v. Regan, 453 U.S. 654, 667, 101 S.Ct. 2972, 2980, 69 L.Ed.2d 918 (1981)). The Court went on to conclude that the statute in question did not limit the President's discretion and was therefore unreviewable.

Notably, Dames & Moore, the case cited by the Court for the proposition that some non-APA statutory claims may still be subject to judicial review, involved review of various Executive Orders and regulations issued pursuant to the IEEPA which nullified attachments on Iranian assets in the United States and suspended claims against Iran following the hostage crisis. While the Court did not address the reviewability of the claims, [FN12] it did indicate that when the President acts under authorization from Congress "the executive action 'would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it.' " Dames & Moore, 453 U.S. at 668, 101 S.Ct. at 2981 (quoting Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637, 72 S.Ct. 863, 871, 96 L.Ed. 1153 (1952)). The Court concluded that the IEEPA did authorise the nullification of attachments but did not directly authorise the suspension of claims. Id. at 675, 72 S.Ct. at 932-33. However, despite this conclusion, *1299 the Court went on to find that due in part to the tenor and breadth of the IEEPA and congressional acquiescence in the practice of claim settlement by executive agreement, the President did not lack the power to settle claims against Iran.

> FN12. In fact, due to the significance of the issues involved, the Court granted certiorari prior to judgment and ordered expedited briefing.

Although the Supreme Court suggested the possibility of judicial review of non-APA statutory claims, it did not indicate, beyond the very narrow and specific instance identified in Dames & Moore, under what circumstances that review might take place. One appellate court has concluded that Dalton does not preclude judicial review of executive action for conformity with an authorizing statute, or any other statute. Chamber of Commerce of U.S. v. Reich, 74 F.3d 1322, 1331 (D.C.Cir.1996). Unlike the actions in Franklin and Dalton where the final action taken was by the President, and

much like the present case, Chamber of Commerce involved an Executive Order which initiated agency regulations where the regulations carried direct and final consequences for the plaintiff. However, the court in Chamber of Commerce speaks boldly about the reviewability of executive action without readily distinguishing between whether such review lies equally for the President as for an executive official. [FN13] In fact, in a footnote the court concedes that the "Dalton Court's hesitancy to review presidential action ... suggests a reluctance to bring judicial power to bear directly on the President. Of course, here we are concerned with the long established non-statutory review of a claim directed at a subordinate executive official." Id. at 1331 n. 4. Indeed, the court goes on to note that in all the cases cited by the Dalton court, "special reasons existed for concluding that judicial review was precluded." Id. at 1331 n. 5. Those reasons involved matters of political discretion and national security. Id.

FN13. The Ninth Circuit on at least one occasion has declined to endorse the Chamber of Commerce decision. Alameda Newspapers, Inc. v. City of Oakland, 95 F.3d 1406, 1419 (9th Cir.1996).

Finally, in United States v. Spewr Optical Research, Inc., 685 F.2d 1075 (9th Cir.1982), the Ninth Circuit, in a case predating Franklin and Dalton, reviewed an Executive Order by President Ford under the IEEPA's predecessor, the TWEA, continuing the EAA export regulations pending expiration of that Act. The Spawrs were convicted of the unlicensed exportation of laser mirrors after the EAA's expiration "when the sole basis for the regulations was the Executive Order." Id. at 1080. Much like plaintiff here, the Spawrs argued on appeal that the government lacked authority to prosecute them because there was no genuine emergency, the regulations were not related to any emergency then in effect, and Congress had intended to let the regulations lapse. Id. Reviewing language very similar to that of the IEEPA, the court found that the statute afforded broad and extensive powers. Id. Noting that in the face of such broad discretion, courts have been wary of reviewing the political considerations involved in declaring or continuing a national emergency, the Spawr court declined to do so as well. Id. However, the court then concluded that "[a]lthough we will not address these essentially-political questions, we are free to review whether the actions taken pursuant to a national emergency comport with the power delegated by Congress." Id. at 1081 (citing United States v. Yoshida International, Inc., 63 C.C.P.A. 15, 526 F.2d 560, 579 (Cust. & Pat.App.1975)). In swift analysis the court went on to find that the regulations were rationally related to the emergency claimed and that Congress did not intend to terminate the regulations. Id. In fact, the court noted that each time the EAA had lapsed previously the President had issued an Executive Order declaring a national emergency to continue the export regulations and "Congress not only tolerated this practice, it expressed approval of the President's reliance on the TWEA to maintain the export regulations." Id. Such has been the case under the IEEPA as well. [FN14] See, e.g., Exec. Order No. 12444, *1300 48 Fed.Reg. 48215 (1983); Exec. Order No. 12730, 55 Fed.Reg. 40373 (1990), reprinted in 50 U.S.C.App. § 1701 at 598 (1991); Exec. Order No. 12924, 59 Fed.Reg. 43437 (1994). Plaintiff notes that in recent years Congress has criticized use of the IEEPA to extend export regulations when the EAA lapses. Plf. Mem. in Opp. at 17 n. 49 (citing statements made by various members of Congress). Be that as it may, it is within Congress' power to change this practice and it has chosen not to.

FN14. In fact, as defendants point out, when the TWEA was amended and the IEEPA enacted (as Title II of the same bill), the House Report on the legislation indicated that while it rejected a suggestion by the committee to make the EAA permanent legislation, the committee expected that in the case of future lapses of the EAA "the authority of Title II of this bill could be used to continue the Export Administration

> Regulations in effect if, and to the extent that, the President declared a national emergency as a result of such lapse according to the procedures of the National Emergencies Act." H.R.Rep. No. 95-459, at 3 (1977).

While the analysis in Spawr is useful given that the facts are strikingly similar to the instant action, this court cannot ignore the skepticism with which the Supreme Court recently has approached judicial review of a presidential exercise of statutory authority absent a constitutional claim. As noted above, this case differs from Franklin and Dalton in that the final action is taken by the agency rather than the President. [FN15] But that does not significantly change the analysis of whether the actions the President took are reviewable. On this score Chamber of Commerce is not illuminating and the Supreme Court's allusion to Dames & Moore remains opaque. Indeed, given that the law is still unsettled on this question and that considerations precluding review do not apply to agencies--thereby allowing plaintiff to seek the same relief from agency action on the basis of a claim that the agency acted in excess of statutory authority--the court favors deference to the executive. In light of the recent Supreme Court decisions in this area, this court concludes that it cannot review whether the President exceeded his statutory authority under the IEEPA to transfer jurisdiction of encryption items to the Commerce Department.

> FN15. Admittedly, in both of those cases review was precluded in large part because the Court found that the authorizing statutes at issue granted broad discretion to the President. However, this action is not so different as to allow a court to review what the Ninth Circuit has found to be the extensive discretion afforded by section 5(b) of the TWEA, which was essentially reenacted as section 1702 of the IEEPA. Both sections 1701 and 1702 provide little guidance with which to judge the actions taken by the President. Where "the Act provides no standards by which to judge the exercise of discretion by the Executive Branch, we cannot subject that exercise of discretion to judicial review." Medina v. Clinton, 86 F.3d 155, 158 (9th Cir.1996) (citing Dalton, 114 S.Ct. at 1728, 511 U.S. at 476-77).

C. Statutory Authority of the Commerce Secretary to Regulate Encryption Items Under the IEEPA

Of critical importance in both Franklin and Dalton was the fact that the President was responsible for the final action under the statutes at issue. "What is crucial is the fact that '[t]he President, not the [Commission], takes the final action that affects' the military installations." Dalton, 511 U.S. at 470, 114 S.Ct. at 1725 (quoting Franklin, 505 U.S. at 799, 112 S.Ct. at 2774-75). Here we have the situation at issue in Chamber of Commerce, where the President's Executive Order initiated the regulatory process and left it to the agency to finalize the rules. "That the Secretary's regulations are based on the President's Executive Order hardly seems to insulate them from judicial review...." Chamber of Commerce, 74 F.3d at 1327; see also Milena Ship Management Co. Ltd. v. Newcomb, 804 F.Supp. 846, 850 (E.D.La.1992) (reviewing agency action taken pursuant to an unchallenged executive order under the IEEPA). Accordingly, this court will examine whether the Commerce Department's regulation of encryption items is consistent with the IEEPA. [FN16]

> FN16. Since the EAA has expired, the "sole basis for the regulations" is the Executive Order, which itself is premised on the IEEPA. Spawr, 685 F.2d at 1080.

[4] To the extent that plaintiff argues that the regulations governing encryption are not a temporary exercise of emergency power, the question really belongs to the legitimacy of the Executive Order in the first instance and the court declines to address it. The declaration of a national emergency is an action that rests with the President and is based on his broad discretion under section 1701 of the IEEPA. Moreover, the question of

employing the IEEPA--or the TWEA before it--to maintain export regulations during lapses in the EAA was essentially laid to rest by the Ninth Circuit in Spawr and by the legislative history of the IEEPA.

> *1301 [I]t is unmistakable that Congress intended to permit the President to use the TWEA to employ the same regulatory tools during a national emergency as it had employed under the EAA. We, therefore, conclude that the President had the authority during the nine-month lapse in the EAA to maintain the export regulations.

Spawr, 685 F.2d at 1082.

[5] The gravamen of plaintiff's ultra vires argument is that the IEEPA does not authorize the regulation of speech, particularly speech that does not involve a foreign interest in property, and that as speech, encryption software fits well within the exemption for personal communications and informational materials in sections 1702(b)(1) & (3).

With respect to whether encryption software fits within the scope of "property in which any foreign country or a national thereof has any interest", the court finds that section 1702(a)(1) is sufficiently broad to allow for many forms of property, both tangible and intangible, and many forms of interest, both direct and indirect. See 31 C.F.R. §§ 500.311, 500.312; see also Spawr, 685 F.2d at 1081 n. 10 (finding that section 5(b) of the TWEA was broad enough to allow regulation "of any property to any foreign country"). Encryption software or other technology comes within this section.

[6] Plaintiff also alleges that the regulations are beyond the statutory authority of the IEEPA because they affect personal communications and informational materials. Section 1702(b)(1) prohibits direct or indirect regulation of "any postal, telegraphic, telephonic or other personal communication" which does not transfer anything of value. As defendants convincingly argue, to the extent this argument is directed at academic discussion of cryptographic ideas, the regulations attempt to exempt such communications--although whether they do so according to the demands of the First Amendment is a separate question. To the extent this argument is directed at cryptographic software generally, it does not appear to fit within this seemingly narrow and simple provision. Nor can it be assured that software would have no value. Indeed, there are potentially billions of dollars at stake in the export of commercial encryption software. See Jared Sandberg, "Judge Rules Encryption Software Is Speech in Case on Export Curbs," Wall St. J., Apr. 18, 1996, at B7. Thus, the regulations do not exceed this statutory provision.

[7] Finally, plaintiff contends that the regulations go beyond the authority provided by section 1702(b)(3) which specifically limits regulation of information or informational materials regardless of format or medium of transmission. Plaintiff argues that the broad scope of this provision precludes regulation of encryption software. In addition, plaintiff contends that by specifically referencing sections 2404 and 2405 of the EAA, and exempting--from the informational materials exemption--items "otherwise controlled for export" under those sections, the court is bound by principles of statutory construction to consider only those items controlled when section 1702(b)(3) was last amended, or April 30, 1994. Plaintiff then concludes that because encryption software fits within the scope of this provision and was not otherwise controlled under the EAA as of April of 1994, it cannot be regulated under the IEEPA.

Defendants contend that section 1702(b)(3) does not expressly provide for software, and that to include software in those items exempted from regulation for their informational value would lead to absurd results. Moreover, defendants counter plaintiff's statutory construction argument and claim that the items exempted from this provision by virtue of being controlled under the EAA are not only those that were on the Commerce Control List as of April of 1994 but any others that have since been added--including the encryption technology at issue here. Defendants also argue that to read

section 1702(b)(3) as exempting encryption software on the basis that it is protected under the First Amendment would be to impose a novel theory of free speech not contemplated by Congress.

As noted above, the IEEPA explicitly excludes any authority

> "to regulate or prohibit, directly or indirectly-... the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless *1302 of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds. The exports exempted from regulation or prohibition by this paragraph do not include those which are otherwise controlled for export under section 2404 of the Appendix to this title, or under section 2405 of the Appendix to this title to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States...."

50 U.S.C. § 1702(b)(3) (Supp.1996).

First, the court must consider whether software-in this case, encryption software-comes within the exception to the exception; if so, then the instant regulations do not exceed their statutory authority. In other words, anything controlled by sections 2404 and 2405 of the EAA may be regulated regardless of its informational content. Under the referenced sections of the EAA the President may "prohibit or curtail the exportation of any goods, technology, or other information subject to the jurisdiction of the United States" for either national security or foreign policy reasons. 50 U.S.C.App. § 2405(a)(1) (foreign policy controls); 50 U.S.C.App. § 2404(a)(1) (national security controls). It is not disputed that Executive Order 13026, by transferring encryption products to the Commerce Control List ("CCL"), subjected them to regulation under sections 2404 and 2405 of the EAA.

The question becomes whether reference to sections 2404 and 2405 of the EAA should be understood to include all items currently on the CCL-in which case the present regulations effectively remove encryption products from the exemption-or whether rules of statutory construction require the court to construe the reference to those sections as including only those items listed at the time section 1702(b) was last amended, or April 30, 1994. A secondary issue complicates this already complicated matter further: since sections 2404 and 2405 do not themselves designate specific items on the CCL, which is governed by regulation, does the construction of the IEEPA with respect to those sections also apply to their implementing regulations?

Plaintiff relies on a canon of statutory construction discussed in Hassett v. Welch, 303 U.S. 303, 314, 58 S.Ct. 559, 564-65, 82 L.Ed. 858 (1938) and Pearce v. Director, Office of Workers' Comp. Programs, 603 F.2d 763, 767 (9th Cir.1979) which holds that without clear congressional indication to the contrary, where one statute adopts provisions of another by specific reference to the provisions adopted (known as a statute of specific reference) the effect is that such adoption takes the provision as it existed at the time of adoption and does not include subsequent amendments; conversely, where a statute adopts the general law in a given area (a statute of general reference), it is construed to adopt that law's subsequent amendments. See 2A Sutherland, Statutory Construction § 51.07 (4th ed.1984). Plaintiff claims that the IEEPA is a statute of specific reference and cannot be read as adopting subsequent changes to sections 2404 and 2405 of the EAA. Plaintiff further supports this position by pointing to the fact that at least one agency has interpreted the "informational materials" provision to exclude items that were, as of April 30, 1994, controlled for export under sections 5 and 6 of the EAA. 31 C.F.R. § 560.315(b) (Office of Foreign Assets Control regulation of Iranian transactions).

Defendants contend that the IEEPA is more like the statute in United States v. Smith, 683 F.2d 1236 (9th Cir.1982), in which the Ninth Circuit read the Youth Corrections Act

("YCA") as not incorporating specific provisions of the general probation statute. The court concluded that while there were persuasive arguments on both sides, the YCA did not really appear to adopt or incorporate the referenced provisions of the probation statute. "Rather, it merely provides that the YCA is not to 'be construed in any wise to amend, repeal, or affect the provisions of' the probation statute." Id. at 1239. According to the court this was not properly a statute of specific reference in which certain provisions of another statute are incorporated into it, but one that "actually emphasizes that these are distinct statutes". Id. Under defendants' reasoning, section *1303 1702(b)(3) of the IEEPA does not incorporate sections 2404 and 2405 of the EAA but rather distinguishes them and as such those sections are to be read with their full and current force.

This court believes that defendants have the better argument. The rules of statutory interpretation are not hard and fast. "A provision which, in terms, however, reads as a specific reference may, in context, be construed as a general reference." United States v. Rodriguez-Rodriguez, 863 F.2d 830, 831 (11th Cir.1989). Such is the case here. Read in context, section 1702(b)(3) excludes rather than incorporates those items covered under the EAA. Moreover, the sections referenced are themselves fairly general and are clearly intended to be fleshed out by regulations suited to meet the changing needs of national security and foreign policy. Given the goals of the IEEPA and the powers it gives the President, it would seem odd indeed for Congress to exclude from the exemption those items the President deems sensitive to the national security under the EAA, but to freeze that list of items as of a certain date. As the court noted in Smith, this "is the more appropriate interpretation in view of the policies that the [statute] is designed to advance. It is proper, and indeed essential, to interpret the words of a statute in the light of the purposes Congress was seeking to serve." 683 F.2d at 1240 (citations omitted). Therefore, because encryption products are currently regulated under sections 2404 and 2405 of the EAA they do not fall within the exemption for informational materials. [FN17]

FN17. Even assuming the exemption excludes from regulation only those items designated before April 30, 1994, many software products were regulated at that time. That being so, there is no support for the contention that software generally would fall within the exemption.

[8] Accordingly, this court finds that the regulation of encryption items is not prohibited by section 1702(b)(3) and therefore does not exceed the statutory authority provided by the IEEPA. It is worth noting at this juncture that this court's rather narrow determination that source code is speech protected by the First Amendment does not serve to remove encryption technology from all government regulation. Both parties exaggerate the debate needlessly. Plaintiff does so by aggrandizing the First Amendment, by assuming that once one is dealing with speech that it is immaterial what the consequences of that speech may be. Defendants do so by minimizing speech, by constantly referring to "mere speech" or "mere ideas" in their briefs and assuming that the functionality of speech can somehow be divorced from the speech itself. This controversy is before this court precisely because there is no clear line between communication and its consequences. While defendants may have the authority to regulate encryption source code, they must nonetheless do so within the bounds of the First Amendment.

II. Prior Restraint [FN18]

FN18. Portions of the court's analysis of prior restraint cases in taken directly from its opinion in Bernstein II, 945 F.Supp. at 1286-90.

A. Analytical Framework

[9] As the Supreme Court has stated, in determining the extent of the constitutional protection afforded by the guarantees of the First Amendment, "it has been generally, if not universally, considered that it is the chief

purpose of the guaranty to prevent previous restraints upon publication." Near v. Minnesota, 283 U.S. 697, 713, 51 S.Ct. 625, 630, 75 L.Ed. 1357 (1931). It is for this reason that the Court has held: "Any prior restraint on expression comes to this Court with a 'heavy presumption' against its constitutional validity." Organization for a Better Austin v. Keefe, 402 U.S. 415, 419, 91 S.Ct. 1575, 1578, 29 L.Ed.2d 1 (1971) (citations omitted).

[10] While prior restraints have often come in the form of judicial injunctions on publication, see e.g., C.B.S. v. Davis, 510 U.S. 1315, 114 S.Ct. 912, 127 L.Ed.2d 358 (1994); New York Times Co. v. United States, 403 U.S. 713, 91 S.Ct. 2140, 29 L.Ed.2d 822 (1971), they are also recognized in licensing schemes. See e.g., FW/PBS, Inc. v. Dallas, 493 U.S. 215, 110 S.Ct. 596, 107 L.Ed.2d 603 (1990); Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750, 108 *1304 S.Ct. 2138, 100 L.Ed.2d 771 (1988). Governments may impose valid time, place and manner restrictions when they are content neutral, narrowly tailored to serve a substantial governmental interest, and leave open alternative channels for communication. See e.g., Clark v. Community for Creative Non-Violence, 468 U.S. 288, 293, 104 S.Ct. 3065, 3068-69, 82 L.Ed.2d 221 (1984). However, "even if a government may constitutionally impose content-neutral prohibitions on a particular manner of speech, it may not condition that speech on obtaining a license or permit from a government official in that official's boundless discretion." Lakewood, 486 U.S. at 764, 108 S.Ct. at 2147.

[11] It is axiomatic that the First Amendment is more tolerant of subsequent criminal punishment of speech than it is of prior restraints on the same speech.

> The thread running through all these cases is that prior restraints on speech and publication are the most serious and the least tolerable infringement on First Amendment rights. A criminal penalty or a judgment in a defamation case is subject to the whole panoply of protections afforded by deferring the impact of the judgment until all avenues of appellate review have been exhausted .....
>
> A prior restraint, by contrast and by definition, has an immediate and irreversible sanction. If it can be said that a threat of criminal or civil sanction after publication "chills" speech, prior restraint "freezes" it at least for the time.

Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559, 96 S.Ct. 2791, 2802-03, 49 L.Ed.2d 683 (1976).

[12] While the Supreme Court has consistently rejected the idea that a prior restraint can never be employed, id. at 570, 96 S.Ct. at 2806, it nonetheless begins with a presumption of invalidity. The danger inherent in prior restraints is largely procedural, in that they bypass the judicial process and locate in a government official the delicate responsibility of passing on the permissibility of speech. See Freedman v. Maryland, 380 U.S. 51, 58, 85 S.Ct. 734, 738, 13 L.Ed.2d 649 (1965) (holding that "a noncriminal process which requires the prior submission of a film to a censor avoids constitutional infirmity only if it takes place under procedural safeguards designed to obviate the dangers of a censorship system".) Freedman sets forth three procedural safeguards that have been used by the Supreme Court to examine licensing schemes: 1) any restraint prior to judicial review can only be imposed for a brief and specified period during which the status quo prevails; 2) expeditious judicial review must be available; and 3) the censor must bear the burden of going to court to suppress speech and once there bears the burden of proof. FW/PBS, 493 U.S. at 227, 110 S.Ct. at 605-06 (citing Freedman, 380 U.S. at 58-60, 85 S.Ct. at 738-39).

[13] When the risks associated with unbridled licensing schemes are present to a significant degree, "courts must entertain an immediate facial attack on the law." Lakewood, 486 U.S. at 759, 108 S.Ct. at 2145.

B. Analysis

In Bernstein II this court held that the ITAR affected an unconstitutional prior restraint on speech due to inadequate procedural

safeguards. Plaintiff contends that the new encryption regulations suffer from identical deficiencies. Defendants do not argue that the effect of the new regulations is notably different from that of the ITAR. [FN19] They do, however, present arguments against some of the reasoning in Bernstein II and to the extent that these arguments are applicable to the current analysis, the court will address them.

FN19. In their motion for reconsideration, defendants concede that the "essential requirements that previously applied to encryption source code under the ITAR would continue under the EAR." Df. Motion for Reconsideration, at 2. The government also acknowledged at oral argument that the issues before the court were basically unchanged.

1. Controls on Encryption Commodities and Software

[14] First, defendants protest that a facial challenge is not applicable here because there is not a "close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of identified censorship risks." Lakewood, 486 U.S. at 759, 108 S.Ct. at 2145. In *1305 Lakewood, a newspaper challenged a city ordinance which required annual permits for newsracks on public property and gave the mayor authority to grant or deny applications for those permits. The Court contrasted laws that are directed at expression, such as one governing the circulation of newspapers, with laws of general applicability not aimed at conduct commonly associated with expression, such as a law requiring building permits. Id. at 760-61, 108 S.Ct. at 2145-46. The former risks self-censorship on the part of those applying for permits and censorship on the part of the decisionmaker. The latter rarely do. See also Freedman, 380 U.S. 51, 85 S.Ct. 734, 13 L.Ed.2d 649 (licensing of films); FW/PBS, 493 U.S. 215, 110 S.Ct. 596, 107 L.Ed.2d 603 (licensing of sexually-oriented businesses). Defendants contend that while licensing schemes that vest unbridled discretion to regulate conduct commonly associated with expression are appropriate for facial attack under prior restraint doctrine, such is not the case here where the activity at issue is the programming of a computer to encrypt information. [FN20] Defendants also cite Roulette v. City of Seattle, 97 F.3d 300, 305 (9th Cir.1996), to support their contention that only laws narrowly and specifically directed at expressive activities are subject to facial challenge. At issue in Roulette was an ordinance that prohibited people from sitting or lying on public sidewalks in certain areas and during certain times. The court, in a pithy opinion, held that "[t]he fact that sitting can possibly be expressive, however, isn't enough to sustain plaintiffs' facial challenge to the Seattle ordinance.... Consistent with this speech-protective purpose, the Supreme Court has entertained facial freedom-of-expression challenges only against statutes that, 'by their terms,' sought to regulate" words or expressive conduct. Id. at 303 (quoting Broadrick v. Oklahoma, 413 U.S. 601, 612-13, 93 S.Ct. 2908, 2915-16, 37 L.Ed.2d 830 (1973)).

FN20. Defendants again spend a great deal of energy arguing that encryption source code is not speech by citing to all the undisputed facts that show its functional capacity--its ability to actually secure communication. Df. Mem. in Support, at 9-10. Defendants argue that just because "a program may be understood by those trained in programming does not negate the functional nature of the program, nor render it a mere 'idea'.... " Df. Mem. in Opp., at 5. Again, the court does not disagree that encryption software is highly functional, but functionality does not remove it from the realm of speech. Just because an idea is functional does not "negate" its expressiveness. Indeed, it is functional speech. Programming is not, as defendants would have it, merely mechanical. It is both an art and a science. "[A] computer program is not just a way of getting a computer to perform operations but rather ... is a novel formal medium for expressing ideas about methodology." Plaintiff. Mem. in Opp.,

from New York Times that national security alone is insufficient without more. Yet that is exactly what both the President and the BXA have offered here as the justification for the regulation: national security and foreign policy interests. Exec. Order No. 13026, 61 Fed.Reg. 58767; 61 Fed.Reg. 68573. Particularly now, when none of the encryption items subject to export controls under the EAR have military applications, a less amorphous rationale is required. [FN21]

FN21. One might make the argument that encryption software could be validly regulated for its "secondary effects," much like adult theaters were in Young v. American Mini Theatres, Inc., 427 U.S. 50, 96 S.Ct. 2440, 49 L.Ed.2d 310 (1976), and Renton v. Playtime Theatres, Inc., 475 U.S. 41, 106 S.Ct. 925, 89 L.Ed.2d 29 (1986), where the Supreme Court upheld zoning ordinances aimed at the secondary effects of such theaters in the surrounding community. However, the secondary effects rationale has never been extended beyond sexually explicit speech. See Boos v. Barry, 485 U.S. 312, 108 S.Ct. 1157, 99 L.Ed.2d 333 (1988) (refusing to apply the rationale to political speech). See also Reno, -- U.S. at ---, 117 S.Ct. at 2342, 138 L.Ed.2d at 893-95, 97 C.D.O.S. at 5002 (considering the secondary effects doctrine in relation to a statute regulating speech on the Internet).

[16] Nor is it necessary that an item be regulated for its content to make the regulations function as a prior restraint on speech. It is enough that they are directed at expressive activity. As the plurality opinion in FW/PBS suggests, even a licensing scheme with a content-neutral purpose must still contain adequate procedural safeguards in order to be constitutional. [FN22] Thus, without deciding whether the regulations are content-based, the court turns to the procedural safeguards afforded under the encryption regulations. As noted above, the Court in FW/PBS *1308 read Freedman to hold that for a licensing scheme to be constitutional, 1) the licensor must make the licensing decision within a specific and reasonable period of time; 2) there must be prompt judicial review; and 3) the censor must bear the burden of going to court to uphold a licensing denial and once there bears the burden of justifying the denial. FW/PBS, 493 U.S. at 227-28, 110 S.Ct. at 605-06 (citing Freedman, 380 U.S. at 58-60, 85 S.Ct. at 738-40). The new regulations, like the ITAR, are woefully inadequate.

FN22. In FW/PBS Justice O'Connor, joined by Justices Stevens and Kennedy, stated: Because we conclude that the city's licensing scheme lacks adequate procedural safeguards, we do not reach the issue decided by the Court of Appeals whether the ordinance is properly viewed as a content-neutral time, place, and manner restriction aimed at secondary effects arising out of the sexually oriented businesses. FW/PBS, 493 U.S. at 223, 110 S.Ct. at 603.

[17] The EAR provides that license applications will be resolved or referred to the President within 90 days. [FN23] 15 C.F.R. § 750.4(a). However, there is no time limit on an application that has been referred to the President. If a license is denied, the agency provides an internal appeals process, 15 C.F.R. Pt. 756, but the only time limit on the appeals decision is that the agency "shall decide an appeal within a reasonable time after receipt of the appeal." 15 C.F.R. § 756.2(c)(1). That decision is final and not subject to judicial review. 15 C.F.R. § 756.2(c)(2); 50 U.S.C.App. § 2412(e); see also United States v. Bozarov, 974 F.2d 1037, 1044-45 (9th Cir.1992) (EAA's preclusion of judicial review does not violate nondelegation doctrine), cert. denied, 507 U.S. 917, 113 S.Ct. 1273, 122 L.Ed.2d 668 (1993). [FN24] And most important, and most lacking, are any standards for deciding an application. The EAR reviews applications for licenses "on a case-by-case basis" and appears to impose no limits on agency discretion. 61 Fed.Reg. 68581 (to be codified at 15 C.F.R. § 742.15(b)). Like the ordinance in Lakewood, where the mayor could deny a permit without any more justification than that it was not in the public interest, nothing in the regulations prevents

the BXA from justifying a denial of an application by stating that it is contrary to national security and foreign policy interests. [FN25] As the Court noted in Lakewood, these are illusory constraints. 486 U.S. at 769, 108 S.Ct. at 2150-51; see also Desert Outdoor Advertising Inc. v. City of Moreno Valley, 103 F.3d 814, 818 (9th Cir.1996) (finding billboard permit requirement unconstitutional because city officials had "discretion to deny a permit on the basis of ambiguous and subjective reasons"). This court has stated previously that while it is mindful of the problems inherent in judicial review of licensing decisions regarding cryptographic software, both with respect to the sophistication of the technology and the potentially classified nature of the licensing considerations, there must still be some review available if the export controls on cryptographic software are to survive the presumption against prior restraints on speech. In this case, for the reasons enumerated, the court concludes that the encryption regulations are an unconstitutional prior restraint in violation of the First Amendment.

FN23. Given the other more obvious deficiencies in the procedural aspects of the regulations, the court does not consider whether 90 days is fast enough given the demands in the field of cryptography.

FN24. To the extent the EAR are authorized by the IEEPA, that statute does not appear to preclude judicial review. Milena Ship Management Co. Ltd. v. Newcomb, 804 F.Supp. 846, 850 n. 2 (E.D.La.1992) (nothing in IEEPA provides clear evidence of intent to preclude judicial review). However, if the EAR are authorized exclusively by Executive Order 13026, that order seems to preclude judicial review. Exec. Order No. 13026, 61 Fed.Reg. 58768.

FN25. As the court discussed in Bernstein II with respect to the ITAR, some of the dangers of a standardless licensing scheme had already been realized. According to the NRC Report, the risk of discriminatory treatment associated with such schemes was reflected in the Report's comments that companies were reluctant to express their full dissatisfaction with the rules and implementation of export controls over cryptographic products for fear that "any explicit connection between critical comments and their company might result in unfavorable treatment of a future application for an export license for one of their products." NRC Report at 4-29.

2. Controls on Encryption Technology

Plaintiff does not distinguish the regulation of encryption technology--as opposed to commodities and software--for the purposes of prior restraint analysis. With respect to vagueness, the only provision he addresses as vague is "technical assistance." 15 C.F.R. § 744.9(a). Defendants allege that plaintiff lacks standing to challenge the controls on technology because they have not been applied to him and any injury is speculative. *1309 Even if plaintiff is found to have standing,-defendants contend that a facial challenge is still inappropriate because United States v. Edler Indus., Inc., 579 F.2d 516, 520 (9th Cir.1978), found that the technical data provisions of the predecessor to the AECA survived constitutional challenge with a narrowing construction.

[18] It does not appear necessary to address the vagueness argument advanced by plaintiff, or any of the other constitutional arguments, as the bulk of the encryption regulations have been adjudged to constitute a prior restraint on speech. The First Amendment does not "render inapplicable the rule that a federal court should not extend its invalidation of a statute further than is necessary to dispose of the case before it." Brockett v. Spokane Arcades, Inc., 472 U.S. 491, 502, 105 S.Ct. 2794, 2801, 86 L.Ed.2d 394 (1985) (citation omitted). The restrictions on technical assistance under the new regulations prohibit a person from providing technical assistance without a license to foreign persons "with the intent to aid a foreign person in the

development or manufacture outside the United States of encryption commodities and software that, if of United States origin, would be controlled for 'EI' reasons under ECCN 5A002 or 5D002." 61 Fed.Reg. 68584 (to be codified at 15 C.F.R. § 744.9). The technical assistance provision also states that the "mere teaching or discussion of information about cryptography" does not establish the requisite intent. 51 Fed.Reg. 68584 (to be codified at 15 C.F.R. § 744.9(a)). However cryptic this provision might be viewed in relation to the more expansive exemptions for educational information and fundamental research elsewhere in the regulations, because it is dependant on the definitions and regulation of encryption commodities and software, it is unenforceable under the court's holding above.

III. Proper Defendants

[19] Plaintiff named three additional defendants in his supplemental complaint--the Departments of Energy ("DOE") and Justice ("DOJ") and the Central Intelligence Agency ("CIA")--because officials from each are now involved in some way with licensing reviews. 61 Fed.Reg. 68585 (to be codified at 15 C.F.R. § 750.3(b)(2)(v)); 15 C.F.R. § 750.4(d)-(e); 15 C.F.R. § 772 (listing committees involved in interagency review and their members). Plaintiff also contends that these agencies are involved with overall jurisdictional decisions as well. Press Release, at 4 (stating that after legislative reauthorization of export controls the Secretaries of Defense and State together with the Attorney General "shall reexamine whether adequate controls on encryption products can be maintained under the provisions of the new statute and advise the Secretary of Commerce of their conclusions as well as any recommendations for action"). Defendants claim that there is no justification for joining every agency that participates in the review process and that the Secretary of Commerce is the only proper defendant.

The court is inclined to agree with defendants. The roles played by the DOE, DOJ and the CIA are limited to consulting and advising the Secretary of Commerce who is responsible for final decisions. Even if those agencies are asked to review any new legislation that may be passed, [FN26] their roles are advisory. Accordingly, any determination against the Secretary of Commerce is sufficient and the DOE, DOJ and the CIA are dismissed as defendants. Furthermore, because the applicable regulations are no longer implemented by the Department of State, the Secretary of State is also dismissed.

FN26. It is not clear from the Press Release accompanying the President's Executive Order 13026 whether the review these agencies are to provide is limited to the enactment of new legislation or whether they will also review the new regulations.

IV. Scope of Relief

[20] Plaintiff requests that in addition to declaratory relief, the court issue a permanent injunction against defendants barring nationwide application of the encryption regulations on the grounds that loss of First Amendment freedoms constitutes irreparable injury, Elrod v. Burns, 427 U.S. 347, 373, 96 S.Ct. 2673, 2689-90, 49 L.Ed.2d 547 (1976), and that he will not be afforded complete relief unless an injunction extends to students, colleagues and others not before the court. Bresgal v. Brock, 843 F.2d 1163 (9th *1310 Cir.1987). Defendants protest that a nationwide injunction is improper because relief should be no broader than necessary, Meinhold v. United States Dept. of Defense, 34 F.3d 1469, 1480 (9th Cir.1994), and because the issues are novel and of public importance. Azurin v. Von Raab, 792 F.2d 914, 915 (9th Cir.1986).

In Bresgal, the Ninth Circuit found in the absence of a certified nationwide class that a district court could still order nationwide relief in order to ensure the prevailing parties were given the relief to which they were entitled so long as the injunction was directed against a party to the action, in that case the Secretary of Labor. 843 F.2d at 1170-71. However, this holding must still be weighed against the rule that an injunction should be

no more burdensome than necessary to afford complete relief. Meinhold, 34 F.3d at 1480 (quoting Califano v. Yamasaki, 442 U.S. 682, 702, 99 S.Ct. 2545, 2558-59, 61 L.Ed.2d 176 (1979)). In this instance the court, particularly given its determination of facial invalidity of the regulations, could indeed order nationwide relief. However, as it did in Bernstein II, the court concludes that because the legal questions at issue are novel, complex and of public importance, the injunctive relief should be as narrow as possible pending appeal. See Asurin, 792 F.2d at 915. While declaratory relief should be sufficient, plaintiff should not fear prosecution for teaching and writing about encryption. Nor should plaintiff have to conduct his scholarly activities under stipulation with the government. Accordingly, defendants are enjoined from enforcing the regulations against plaintiff or against anyone who seeks to use, discuss or publish plaintiff's encryption program.

V. Effect of Previous Order

Defendants ask the court to vacate its order in Bernstein II as the controversy has shifted to the new regulations and Category XIII of the , USML no longer covers plaintiff's software. Plaintiff argues the court should reaffirm its previous order because the President left open the possibility that jurisdiction would be shifted back to the Department of State if export controls under the Commerce Department prove inadequate. The likelihood of the jurisdiction being transferred back to the State Department seems too remote to justify maintaining an order that no longer applies to the controversy before the court. While the government cannot avoid the constitutional deficiencies of its regulations by rotating oversight of them from department to department, the court does not believe that such was the intent here. Moreover, should the President direct that export controls on encryption be regulated under the ITAR once more, plaintiff can come back before this court at that time. However, given the continuing validity of the rationale in Bernstein II to the present order, neither is it necessary to vacate that decision. Accordingly, the court's holding in Bernstein II, in so far as it relates to the ITAR, is hereby superseded by the present order.

CONCLUSION

For the aforementioned reasons,

1) plaintiff's motion for summary judgment is GRANTED in part and DENIED in part in accordance with the foregoing;

2) defendants' motion for summary judgment is DENIED in part and GRANTED in part in accordance with the foregoing;

3) the Departments of State, Energy, Justice and the Central Intelligence Agency are dismissed as defendants;

4) the court's holding in Bernstein v. United States Dept. of State, 945 F.Supp. 1279, is superseded by this order;

5) the court declares that the Export Administration Regulations, 15 C.F.R. Pt. 730 et seq.(1997) and all rules, policies and practices promulgated or pursued thereunder insofar as they apply to or require licensing for encryption and decryption software and related devices and technology are in violation of the First Amendment on the grounds of prior restraint and are, therefore, unconstitutional as discussed above, and shall not be applied to plaintiff's publishing of such items, including scientific papers, algorithms or computer programs;

6) defendants are permanently enjoined from doing or causing to be done the following acts:

*1311 a) further and future enforcement, operation or execution of the statutes, regulations, rules, policies and practices declared unconstitutional under this order, including criminal or civil prosecutions with respect to plaintiff or anyone who uses, discusses or publishes or seeks to use, discuss or publish plaintiff's encryption program and related materials described in paragraph 5) of this order; and

b) threatening, detaining, prosecuting, discouraging or otherwise interfering with plaintiff or any other person described in

paragraph 6) above in the exercise of their federal constitutional rights as declared in this order.

IT IS SO ORDERED.

END OF DOCUMENT

Senator ASHCROFT. Tim Casey is the chief technology counsel for law and public policy with MCI. He holds both law and engineering degrees and has a great deal of experience dealing with high-tech legal issues for MCI.

Mr. Casey, we are glad that you have come to the committee, and would you please begin your testimony?

STATEMENT OF TIM D. CASEY

Mr. CASEY. Thank you. On behalf of MCI, thank you, Mr. Chairman, for inviting me to testify before your subcommittee on this very important issue.

MCI believes that controls on the use of strong encryption, including key recovery systems, are contrary to the best interests of the American people for at least three reasons. Such controls, one, could harm the ability of American businesses to compete with foreign companies for foreign and domestic customers; two, undermine the enormous potential of the Internet, including global electronic commerce, to improve the lives of all Americans; and, three, violate the constitutional rights of privacy and abrogate the protections of the fourth and fifth amendments.

But perhaps even more important than those considerations, there are a number of practical problems associated with any key recovery system that render them futile or even counterproductive to even attempt. Companies such as MCI are concerned that encryption controls will negatively impact our ability to compete with multinational carriers for multinational customers.

MCI offers customized Internet products such as electronic commerce tools and customized browsers that incorporate encryption tools. Because foreign carriers from countries without encryption controls will offer strong encryption to which no government entity holds the keys, we believe that potential customers seeking the highest level of protection will choose their products over ours.

In addition to competitive business concerns raised by controls on strong encryption, the enormous potential of the Internet, including Internet-based global electronic commerce, could be undercut by the Government's effort to limit online privacy. Without strong encryption and severe limits on the Government's ability to access Internet communications, people can lose confidence in the Internet and fail to make use of its full potential. This could destroy the great potential of the Internet to bring new and better services to people, to enhance the efficiency of our economy, and to further strengthen our democracy.

The FBI's proposal for key recovery, in general, and its recent call to include domestic controls on the use of strong encryption, in particular, raise serious questions about the people's right to privacy under the Constitution, although that has clearly already been pointed out by the fellow speakers. As a practical matter, while law enforcement insists that its access to private communications will be limited in scope and possibly subject to properly obtained warrants, the American people are well aware that private efforts to hack into computer systems, including the Internet, are tenacious and pervasive. As a result, providing law enforcement with a key to every communication on the Internet will surely lead to an increase in abuse of those keys by private parties.

Numerous newspaper articles report Americans' concerns regarding the unauthorized use of their personal information. People are increasingly using encryption to protect e-mail and data files. And perhaps in response to the questions earlier about why more people aren't using it, a lot of the programs that have been developed today are not the easiest in the world to use, and I think as the technology becomes more prevalent and available, simpler forms of encryption tools will be allowed and people will then begin to use them more frequently.

Neither the Government nor a trusted third party can guarantee that personal information will not be misused under the key recovery proposals. It has been widely reported that once someone's credit card report, medical history, or other sensitive information has been misused, the consequences can be grave and the misuse difficult or impossible to correct. The very viability of Internet commerce and the integrity of its communications are dependent on the unobstructed use of superior encryption products.

Many consumers are still very wary about purchasing products and services via the Internet, fearful that their credit card numbers could be appropriated. Businesses are rightly worried about threats to the confidentiality and authenticity of their online communications and transactions. Strong encryption can significantly mitigate these concerns by affording individuals and companies on a multinational basis protection from computer crimes and unauthorized access.

As a related matter, limiting privacy on the Internet may bolster the plans of some to impose a new and unreasonably strict copyright regime in cyber space. Providers like MCI may be forced to monitor and/or block the communications of individuals and businesses in a fruitless effort to identify potential copyright infringements. Technical impossibility and practical concerns aside, such monitoring or blocking would invade the privacy of every Internet user.

I certainly do not advocate the violation of copyright laws. However, denying people the right to keep their communications private from the Government and Internet service providers or copyright owners alike is not the way to fight crime and not the way to protect valuable information. In fact, strong encryption can actually help fight crime and protect copyrights and other intellectual property. By ensuring the security of financial transactions, for example, strong encryption can help reduce white collar crime. In addition, strong encryption provides an inexpensive methods for authors and other creators to protect against the theft of copyrighted works on the Internet.

In considering both domestic restrictions and export controls of strong encryption, I want to make an important point about Internet domain names. Domain names ending with the ".com" designation are available to any domestic or foreign company. It can be used by computers anywhere in the world. The typical Internet user is not aware of the location of the domain he or she is accessing.

To take one example, the Government of Singapore has monitored and may still be monitoring all Internet communications entering that country. As a result, the communications of Internet

users around the world accessing the ".com" domain residing in Singapore could be exposed to the watchful eye of that local government. The only way to ensure the highest level of privacy throughout the Internet is to ensure that the strongest encryption is available in the United States for sale or export and to discourage the use of encryption controls abroad.

In addition to all these concerns, practical limitations on the effectiveness of key recovery suggest that its use does not justify the cost to individual privacy. Put simply, key recovery will not work to solve the anti-criminal issue that it is primarily based upon. First, encryption users employing a two-step key process can require a password, often called a challenge phrase, to decrypt the key to an encrypted message. As a result, a stored key without its corresponding password would not function or help law enforcement.

Another type of encryption growing in popularity is the split key method. These systems require a combination of keys to reconstruct the real key originally used to encrypt a message. Because such second-level protections can be modified at the will of the user, stored keys would quickly become worth less than the cost of administering them. Furthermore, common sense suggests that among the most diligent users of such methods would be criminals bent on hiding their communications from the authorities. No matter what system we come up with, there will always be a smarter criminal out there who can defeat it.

MCI recognizes the need to be tough on crime, but doing so should not come at the expense of privacy or fail to make practical sense. The American people are making it increasingly clear that privacy is at the forefront of their concerns. To any suggestion that privacy concerns are exaggerated, I would point to the countries around the world that currently impose controls on the use of encryption. They include Belarus, China, Pakistan, and Russia. I would ask the committee members if you believe the American people want the United States to join that list of countries.

I believe that strong encryption is the key to privacy on the Internet and that such privacy, in turn, is the key to realizing the enormous potential of the Internet and global electronic commerce. MCI has watched the debate over encryption labor on for years without progress. We believe that the time has come to embrace an approach supportive of innovative, strong self-regulation rather than continuing to pursue an elusive compromise between industry and law enforcement.

Thank you again for allowing me to testify today and I would be happy to answer any questions you might have.

Senator ASHCROFT. Thank you, Mr. Casey.

[The prepared statement of Mr. Casey follows:]

PREPARED STATEMENT OF TIM D. CASEY

I. INTRODUCTION

MCI believes that controls on the use of strong encryption, including key recovery systems, are contrary to the best interests of the American people for at least three reasons. Such controls could: (1) harm the ability of American business to compete with foreign companies for foreign and domestic customers; (2) undermine the enormous potential of the Internet, including global electronic commerce, to improve the lives of all Americans; and (3) violate the constitutional right to privacy and abro-

gate the protections of the 4th and 5th Amendments. In addition to these important considerations, there are a number of practical problems associated with key recovery systems that render them futile or even counter-productive.

II. ENCRYPTION CONTROLS ARE CONTRARY TO AMERICA'S BEST INTERESTS

1. Impact on U.S. business

Companies like MCI are concerned that encryption controls will negatively impact our ability to compete with multinational carriers for multinational customers. MCI offers customized Internet products—such as World Wide Web browsers—that incorporate encryption tools. Because foreign carriers from countries without encryption controls will offer strong encryption to which no government entity holds the keys, we believe that potential customers seeking the highest level of protection will choose their products over ours.

By limiting the sale and use of domestically developed U.S. encryption technology abroad, current export controls endanger America's technological competitiveness and its overall economic security. If those in the international marketplace cannot obtain strong encryption products from U.S. firms, they will increasingly turn to foreign suppliers—threatening America's edge in the critical sectors of computer technology and telecommunications. In addition, one of several legislative versions promoted by federal authorities now pending in the U.S. House of Representatives would prohibit domestic manufacturing, sale or importation of any encryption product or service, unless the government is given immediate access to the plain text of communications and stored files so that they can be immediately read without the knowledge of the user. We believe that this requirement would have a chilling effect on our ability to gain new customers and retain our current ones.

2. Potential of the Internet and global electronic commerce

In addition to the specter to American business raised by controls on strong encryption, the enormous potential of the Internet, including Internet-based global electronic commerce, could be undercut by the government's efforts to limit online privacy.

Anyone who once doubted the Internet's potential to transform the daily lives of all Americans, must now see that the Internet has already revolutionized the way millions of people communicate, conduct business, and access information. Without strong encryption and severe limits on the government's ability to access Internet communications, people may lose confidence in the Internet and fail to make use of its full potential. This could destroy the great potential of the Internet to bring new and better services to people, enhance the efficiency of our economy, and further strengthen our democracy.

We stand on the brink of a a great change in the way people and companies conduct business around the world. Electronic commerce will create efficiencies in the cost of doing business, open new markets, and bring new products and services to all people. But this promise will never be fulfilled if the average citizen feels his or her privacy is not secure on the Internet. As a recent front-page Washington Post article reports, of the millions of people already using the Internet, growing numbers are turning to encryption and other methods to protect their privacy online.

3. Constitutional issues

The FBI's proposal for key recovery in general, and Director Freeh's recent call to include domestic controls on the use of strong encryption in particular, raise serious questions about the people's right to privacy under the Constitution.

I urge the Committee Members to parse the words of the 4th Amendment very carefully in considering the constitutionality of controlling strong encryption. The 4th Amendment requires that a warrant particularly describe the places to be searched or the things to be seized. I ask the Committee Members to consider the extent to which key recovery abrogates this important limit on the government's authority. By the very nature of a proposal to store keys in advance, can the "places to be searched" and the "things to be seized" be particularly described?

The 5th Amendment's command is very simple: "No person shall * * * be deprived of life, liberty, or property without due process of law." I suspect that most Americans would consider the keys to their encryption communications and stored data to be their personal property. By requiring the surrender of all keys to all communications and stored data, the American people may feel that their government seeks to deprive them of that property without due process.

As a practical matter, while law enforcement insists that its access to private communications will be limited in scope and subject to properly-obtained warrants, the American people are well aware that private efforts to "hack" into computer systems—including the Internet—are tenacious and pervasive. As a result, providing

law enforcement with a key to every communication on the Internet will surely lead to an increase in abuse of those keys by private parties.

III. THE AMERICAN PEOPLE'S STRONG INTEREST IN PRIVACY

The Post article reports that the American people are becoming increasingly frustrated with unauthorized use of their personal information. The measures people are using to protect that information increasingly include encryption of e-mail and dats files. It is important to understand that a compromise in privacy—even if limited and controlled as the government promises—ia a compromise nonetheless. Neither the government nor a "trusted third party" can guarantee that personal information will not be misused under the key recovery proposals. It's been widely reported that once someone'a credit report, medical history, or other sensitive information haa been misused, the consequencea can be grave, and the misuse difficult or impossible to correct.

A recent survey also provides atrong evidence of the people's serious concern with online privacy matters. So leery are Americana of privacy on the Internet, that 40 percent of the 20,000 respondents to a survey by the Georgia Institute of Technology reported that they have given false personal information when registering at a website. By way of comparison, only 8 percent of those surveyed reported that they were concerned enough about "spamming"—or unsolicited, bulk e-mail—on the Internet to support a legislative solution. This is particularly striking because spamming is widely considered to be one of the biggest problems on the Internet.

The very viability of Internet commerce and the integrity of its communications are dependent on the unobstructed use of superior encryption products. Many consumers are still very wary about purchasing products and services via the Internet, fearful that their credit-card numbers could be appropriated or their privacy compromised. Businesses, moreover, are rightly worried about threats to the confidentiality and authenticity of their online communications and transactions. Strong encryption can aignificantly mitigate these concerns by affording individuals and companies protection from computer crimes and unauthorized access. And in doing so, encryption can facilitate and speed the realization of the Internet's enormous economic and social potential.

IV. COPYRIGHT LIABILITY AND PRIVACY

As a related matter, limiting privacy on the Internet may bolster the plans of some to impose a new and unreasonably strict copyright regime in cyberspace. Providers like MCI may be forced to monitor and/or block the communications of individuals and busineases in a fruitless effort to identify potential copyright infringements. Technical impossibility and practical concerns aside, such monitoring or blocking would invade the privacy of every Internet user.

As explained, the American people have the right to be secure in their communications. I certainly do not advocate the violation of copyright laws; however, denying people the right to keep their communications private—from the government and Internet service providers alike—is not the way to fight crime, and not the way to protect valuable copyrights.

In fact, strong encryption can actually help fight crime and protect copyrights and other intellectual property. By ensuring the security of financial transactions, for example, strong encryption can help reduce white collar crime. In addition, strong encryption provides an inexpensive method for authors and other creators to protect against the theft of copyrighted worka on the Internet.

V. INTERNET DOMAIN NAMES

In considering both domestic restrictions and export controls of strong encryption, I want to make an important point about Internet domain names. Domain names ending with the ".com" designation are available to any domestic or foreign company, and can be used by computers anywhere in the world. The typical Internet user is not aware of the location of the domain he or she is accessing. To take one example, the government of Singapore has monitored and may still be monitoring all Internet communications entering that country. As a result, the communications of Internet users around the world accessing a ".com" address residing in Singapore could be exposed to the watchful eye of that local government. The only way to ensure the highest level of privacy throughout the Internet is to ensure that the strongest encryption is available in the U.S. for sale or export and to discourage the use of encryption controls abroad.

VI. PRACTICAL PROBLEMS WITH KEY RECOVERY

In addition to all these concerns, practical limitations on the effectiveness of key recovery suggest that its use does not justify the cost to individual privacy. Put simply, key recovery will not work to solve the anti-criminal issue that it is primarily based upon. First, encryption users employing a two-step key process can require a password—often called a "passphrase" or "challenge phrase" (which can itself be encrypted)—to decrypt the key to an encrypted message. As a result, a stored key—without its corresponding password—would not function.

Another type of encryption growing in popularity is the split-key method. These systems require a combination of keys to reconstruct the "real" key originally used to encrypt a message. Because such second-level protections can be modified at will by the user, stored keys would quickly become worth less than the cost of administering them. Furthermore, common sense suggests that among the most diligent users of such methods would be criminals bent on hiding their communications from the authorities.

I am unaware of any key recovery system that puts the keys in the hands of users that could not be easily defeated by criminals, even those whose only crime is circumvention of encryption control laws. Centralized systems can be imagined by which, for example, a corporate computer would produce and issue keys to users. I feel strongly, however, given the American people's concern with online privacy, that they will want to choose encryption systems in which they create and manage their own keys. And I'm certain that any proposal forcing companies like MCI to issue and store its customers' keys would contribute to the competitive disadvantage created by encryption controls in general.

VII. CONCLUSION

MCI recognizes the need to be tough on crime; but doing so should not come at the expense of privacy. The American people are making it increasingly clear that privacy is at the forefront of their concerns. To any suggestion that privacy concerns are exaggerated, I would point to the countries around the world that currently impose controls on the use of encryption. They include: Belarus, China, Pakistan, and Russia. I would ask the Committee Members if you believe the American people want the United States to join that list of countries.

I believe that strong encryption is the key to privacy on the Internet, and that such privacy, in turn, is the key to realizing the enormous potential of the Internet and global electronic commerce. MCI has watched the debate over encryption labor on for years without progress. We believe that the time has come to embrace an approach supportive of innovative, strong self-regulation rather than continuing to pursue an elusive compromise between industry and law enforcement.

Senator ASHCROFT. Let me just say that as I ask questions, I would be pleased if those of you to whom the question is not directed—feel free to answer the question anyhow because it is in my best interest to try and have as much information and analysis as I can.

Professor Sullivan, it appears that the Justice Department has argued that the fourth amendment problem is avoided when the Government forces an individual to hand over something to a third party rather than to the Government directly. Do you agree with that or do you have a comment on that?

Ms. SULLIVAN. With respect, Mr. Chairman, I don't think that is correct. I think that if the Government uses private agents to accomplish unconstitutional ends, it can't cure the problem by outsourcing the dragnet. A dragnet is a dragnet even if it is outsourced. The problem here really arises from compelling a search, executing a search at the time that the key has to be given up to third parties, and is no answer to that to say that the fourth amendment will be complied with at a later time when somehow probable cause or reasonableness has been established.

Mr. EPSTEIN. In fact, I thought that Mr. Litt made a fatal concession during his testimony to you when he said, in effect, the search takes place at the time that the key is turned over, not at the time

that the warrant is sought for the information guarded by the key. If that is true, then you have to have the warrant requirement and the probable cause requirements and particular description requirements satisfied at the early stages. And if you ever wanted to talk about a proverbial fishing expedition, this is it. You have billions of pieces of information that will be compromised and you may be looking at a thousand of them over the entire course of their lifetime.

Senator ASHCROFT. Professor Epstein, you mentioned in your written commentary the issue of a taking by Government when something is mandated by way of a key. Would you care to comment on that?

Mr. EPSTEIN. I would be delighted to. The takings issue is, of course, one that lurks in the background of all of these cases, and the precise question you have to worry about is the Government takes the key, puts it in the hands of the third-party agent and it is lost or stolen from that agent. The question is who is going to bear the risk of loss associated with the compromised data which takes place because of that loss or that theft.

Under standard law, what you would try to do is figure out what the optimal risk allocation arrangement is between a bailee of the property—in this case, the key—and the owner of the safe. And the usual rule allocates that loss in accordance with the distribution of benefits and costs. In this case, the Government insists it is for its benefit and it recognizes that it poses a cost on the individual who is forced to turn the key over. So if you were just using standard private law analogies, the risk of loss caused by a third party defalcation would always fall on the Government.

What is striking about these cases is the losses here are immunized from Government compensation, and then the issue is whether or not the deviation from the common law rules on liability with respect to the loss of property constitutes a taking. Academically, I have no doubt that that ought to be the case. In terms of current doctrine, it is a bit more clouded. What happens under current law is the Government may be able to plead some form of sovereign immunity or it may be able to say that the taking was by a third party and not by us.

I think that these are pretty thin verbal distinctions, but even if they are correct, this is a committee which is concerned with property rights as well as with the Constitution and one of the costs that we have to worry about in putting this program forward is, in effect, the cost of loss for which the Government will not assume responsibility and from which it will insulate all third parties from responsibilities.

These are social losses. If they are uncompensated, the standard economic theory applies. If the Government is allowed to externalize the costs of certain activities, it will engage in too much of those activities. That is as true of searching and seizing in criminal investigations as anything else.

The right question to ask Mr. Litt, if he were here, is as follows. If we gave you a large budget, how much would you spend on insurance for losses and how much would you spend on some other systems? My guess is they would not want to fund the losses. They want to keep them off-budget. If put on budget, they would change

their behaviors. And since that is the case, we ought never to allow them to start down this dangerous path to begin with.

Senator ASHCROFT. Ms. Cohn, you bring an interesting and compelling analysis in terms of free speech. Apparently, Government will allow us to speak in codes domestically, but if we get close to the border, our free speech is inhibited. Is that your argument that if you stand too close to Canada, you can't speak the same things that you could if you were in the heart of the Midwest?

Ms. COHN. Well, it is certainly a piece of it, and there is Supreme Court doctrine and ninth circuit doctrine, which is where I practice, that does say that your first amendment right to speak includes your first amendment right to speak to foreigners and that the first amendment doesn't stop at the borders in terms of Americans' rights. And so we think that there is a problem when the Government says, well, you can speak all you want to other Americans, but if you want to try to speak to foreigners, we are going to make sure that you speak in a language we can understand.

It is interesting to me because one of the great tools used in World War II were the Navajo code talkers, and they were chosen precisely because it was such an obscure language that nobody outside the United States was thought to be able to understand it. It appears that that was the case, since their codes were never broken. The idea that the U.S. Government is essentially saying, well, you know, you Navajos have to speak in English now, is, I think, severely problematic to the first amendment.

Ms. SULLIVAN. If I could just add to that, the right to speak also entails the right not to speak, and the Supreme Court has recognized that sometimes the right to speak anonymously is protected by the first amendment. Indeed, it recently held that a woman trying to influence her fellow citizens of a town not to vote for a school board levy had a right to send out pamphlets and try to influence their vote without signing those documents. And in the course of the opinions striking down the law that would have made her reveal her identity, the Court noted that the Framers often spoke with pseudonyms. Publius wrote the Federalist Papers, and that pseudonym was responded to by other pseudonyms from the anti-Federalists, Cato and the Federal Farmer, and so forth.

Justices as diverse otherwise as Justice Stevens and Justice Thomas agree that the right to speak anonymously is protected by the first amendment. If there is a right not to have to reveal your signature on a document, it would follow, it would seem, that if you wanted to keep the content of the document private, that ought to be allowed as well. If Paul Revere wants to say "one if by land and two if by sea" and not reveal the meaning of that signal, that, I think the Framers' generation understood, was a form of speech that perhaps needs to be protected by this right of anonymity.

Mr. EPSTEIN. I would say that there are two issues and the Justice Department has managed to confuse them. The first is what counts as speech, and the second, what counts as a justification for the limitation of speech. I think the argument that a publication of a book which tells people how to encrypt information is not speech is simply fact-specific. The real serious question is whether or not the security risk is sufficiently grave that you could justify

the restriction under something like the clear and present danger doctrine.

What we have heard from everybody on this panel is that we have a very porous world out there and information which allows you to achieve the same result is already available from countless sources, and if it is not available, it will soon be made available from foreign sources. So it seems to me that the size of the Government interest is going to be extraordinarily weak.

Therefore, in order to avoid the question of being explicit with their justifications, what they try to do is to pretend that something which isn't the case is the case, namely that speech is not implicated, so that the issue of justification never arises. And I think that that is just burying your head in the sand and that a much more candid approach would say, yes, when you are dealing with export arrangements, the Government issues may be somewhat stronger than they are in the domestic situation. But even if you were to concede a differential standard, I don't think you get anything close to the kinds of restrictions here, particularly since any export controls will surely inhibit the development of the national market by virtue of the fact that virtually all of our customers have worldwide subsidiaries and have to enter into regular commerce with foreign nations.

Senator ASHCROFT. So that it is hard to have a narrowly tailored, effective remedy when there are robust encryption devices proliferating all around the world?

Mr. EPSTEIN. Yes. Let me just give you an alternative proposal. You try to figure out what the cost of this monstrosity is going to be and then ask yourself whether or not, if you took general revenues, devoted them all to the FBI and law enforcement and kept them to traditional means—whether they would be better off with those additional revenues than with these play toys. And I think the answer to that question is yes, and so I think what we are doing is we are going down the wrong road in this particular area.

And I would stress that I think it is a business judgment and a political judgment, as well as a constitutional judgment, and if they all line up in the same way, I don't think that we have a particularly vexatious choice to make.

Senator ASHCROFT. Mr. Casey, could you explain how efforts to impose liability on online third parties threatens the privacy interests of end users?

Mr. CASEY. Well, there are a number of ongoing efforts both in the United States and in the EC to attempt to regulate various forms of content being transmitted over the Internet. Perhaps the most notable one in the United States has to do with efforts both in the House and in the Senate to restrict copyright transmissions over the Internet so that illegal or infringing copyrighted works cannot be transmitted.

And as part of that effort, it has been suggested that the service providers who merely act to transport those works from place to place be required at some point in time when technology perhaps becomes available to monitor for infringing works on the Internet, to review those works, and to make a determination as to whether or not they are infringing and should therefore be stopped.

And, of course, the only way that you can make a subjective decision like that is to actually look at whatever material it was that was being transported. And so if you, for example, have encryption, that becomes impossible because not only is it impossible to try to stop the transmissions, monitor them and look at what they are and make a decision about it, but is also impossible if the works have been encrypted. So we have laws going in opposite directions.

Not only should we not have monitoring requirements for Internet traffic, but we should also encourage the use of encryption so that the very works that are trying to be protected can be protected by the people who develop such works. And this is also an issue in many other areas where it involves other forms of content that people would like to have regulated and controlled in some fashion.

Senator ASHCROFT. Professor Epstein.

Mr. EPSTEIN. Yes. I think it is very important that we keep in this particular area the same distinctions that we make, for example, under the general Telecommunications Act, a strong distance between those people who carry content, but don't examine it—that is, common carriers on the one hand and broadcasters who are responsible for figuring out what the content is on the other.

The moment you start to impose on a common carrier the obligations that are associated with the management of content, it seems to me that what you do is you impair their operations and you reduce the confidence that they could extend to other individuals that they will act merely as a conduit in the wire. Instead, what happens is they become the cogenitor of the information. The only people I think who ought to take that particular role on are those who assume it voluntarily, and if a common carrier wants to do it, let it do it from a separate division, and so forth, where it clearly articulates some standards.

But I think that the general rule on liability is quite clear, which is to the extent that you are a common carrier engaged in the transmission of information, you are not responsible for the content unless somebody brings it home to you and you have an opportunity to stop it. So a lending library, for example, would be innocent of any responsibility for the books that it lends until the Government could show quite specifically why this one ought not to distribute it. It works fine in other areas. I don't see any reason to deviate from that rule.

Senator ASHCROFT. Let me just say how much I have appreciated the contributions you all have made.

Senator Patrick Leahy of Vermont is an active participant in the debate on these issues and he has asked that we submit for the record remarks of his. And without objection from the committee and since no one else is here to object, I think I can safely assume that I will include those remarks.

[The prepared statement of Senator Leahy follows:]

PREPARED STATEMENT OF SENATOR PATRICK LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Cryptography is important for our economy, our national security and our privacy, and it will only become more critical with our increasing reliance on computers, computer networks and other digital communications and electronic media. Even if many of us still struggle to understand how encryption works, appreciating the im-

portance of this technology is an imperative of our inexorable transition into what we call the Information Age.

PRIVACY

Some have tried to simplify the encryption debate as one in which you are either for law enforcement and national security or for Internet freedom. Characterizing the debate in these simplistic terms is neither productive nor accurate. This is not a black-and-white issue. As with other new and advanced technologies that engage both law enforcement and civil liberties interests, the solution in this policy debate will only be reached by balancing all legitimate interests. The starting point is our Constitution and the Bill of Rights, which confirms our right to speak freely, associate with whom we wish, to refuse to incriminate ourselves, and to be left alone.

We hear almost daily reports about the threats to privacy from the growth of interconnected computer networks and computer databases. The exponential growth in use of the Internet and similar interactive communications technologies by Americans to obtain critical medical services, to conduct business, and to be entertained and communicate with their friends raises special concerns about the privacy and confidentiality of those communications. Encryption technology offers an effective way to ensure that only the people we choose can read our communications or our e-mail, review our medical records, or take money out of our bank account. For those who want to protect the fruits of their intellectual endeavors, encryption also provides a technical means to enforce yet another important constitutional right, the copyright.

In some places in the world, protecting the confidentiality of encrypted files can be a matter of life and death. I have read horror stories sent to me over the Internet about how human rights groups in the Balkans have had their computers confiscated during raids by security police seeking to root out the identities of people who have complained about abuses. Thanks to the PGP encryption software, the encrypted files were undecipherable by the police and the namea of the people who entrusted their lives to the human rights groups were safe.

I congratulate Chairman Ashcroft and the Ranking Member, Senator Feingold, for convening this hearing and providing a forum to discuss the important privacy and constitutional interests at stake in the encryption debate. How we resolve this debate today will have important repercussions for the exercise of our constitutional rights tomorrow. Every American, not just those in the software industry and not just those in law enforcement agencies, has a stake in the outcome.

FBI "WISH LIST"

At the heart of the encryption debate is the power this technology gives computer usera to choose who may access their communications and stored records, to the exclusion of all others. For the same reason that encryption is a powerful privacy enhancing tool, it also poses challenges for law enforcement. Law enforcement agencies want access even when we do not choose to give it.

The FBI has made clear that law enforcement will settle for no less than immediate access to the plaintext of encrypted communications and stored data, and, absent industry capitulation, will seek legislation to this effect. Indeed, while much of this debate has focused on relaxation of export controls, the FBI has upped the ante. Recognizing that the encryption genie is out of the bottle, the FBI now wants to stuff it back in with import restrictions and domestic controls on encryption.

In response to written questions I posed to the FBI in connection with the Judiciary Committee's encryption hearing on June 25, 1997, the FBI stated:

"Without the adoption of legislation which provides that encryption products manufactured or imported into the U.S. include features that allow for the immediate access to the 'plaintext' of encrypted criminal-related information (both transmitted and stored), pursuant to lawful court order, investigations and subsequent prosecution of criminal activity will continue to be thwarted * * * [I]f the current voluntary efforts are not successful, * * * it is the responsibility of the FBI * * * to seek alternative approaches to alleviate the problems caused by encryption. This would include legislative remedies which effectively address law enforcement concerns regarding the import of robust encryption products, as well as encryption products manufactured for uae in the U.S." (Emphasis supplied).

The Administration's recent letter of March 4, 1998, from the Vice President is fully consistent with this position. While indicating that the Administration prefers a "good faith dialogue" and "cooperative solutions" over "seeking to legislate domestic controls," the latter approach is nowhere ruled out.

LEAHY ENCRYPTION BILLS

Our country is certainly not alone in grappling with the tension between what encryption has to offer for privacy and confidentiality, and the challenge thia poses for public safety. The Organization For Economic Co-Operation and Development (OECD) recently issued a report on Cryptography Policy that summarizes many of the issues that need to be addressed. For example, if lawful access is to be preserved to encrypted information, how should this be done? As the OECD noted, "other issues that may need to be addressed include where keys will be stored, who will be allowed to hold keys, and what will be the responsibilities and the liabilities of keyholders."

At the beginning of this Congress I introduced with Senator Burns two encryption bills, one of which, the "Encrypted Communications Privacy Act", S. 376, proposes answers to these questions that our society and others around the world are facing. This bill is pending in the Judiciary Committee and waa endorsed most recently by the U.S. Chamber of Commerce.

This legislation would ensure the right of Americans to choose how to protect their privacy and promote the global competitiveness of American companies. It calls for an overhaul of our export restrictiona on encryption and prohibits a government-mandated key escrow encryption system. For those business or individual users who choose to use an encryption method with a recoverable key stored with another party, the bill would set up stringent procedures for law enforcement and foreign governments to follow to obtain decoding keys or decryption assistance to read the plaintext of encrypted communications obtained under court order or other lawful process.

There may be a market for a user-friendly, cost-effective form of key recovery with user choice on key holder, so that businessea and individuals can recover encrypted data that is important to them. Law enforcement access to those keys should be accommodated subject to appropriate procedurea to safeguard privacy and civil liberties. That is the thrust of my encryption bill.

By contrast with the voluntary, market-driven approach of my bill, the Administration has so far insisted on burdensome regulations of key recovery systems, guaranteed access to both encrypted communications and stored filed, access to keys by both domestic and foreign law enforcement agencies on a minimal showing, and no notice of key disclosurea to the owners of those keys. These conditions pose significant obstaclea to a market-driven approach in the development of key recovery aystema.

Americans should be free to choose any encryption method that suits their needs to protect the privacy of their online communications and computer files. Government efforts to dictate to Americans the type of encryption they should use will be fruitless. If consumers have no need for the government-sanctioned encryption, they simply will not use it. The marketplace has a decisive voice in this issue, as the failure of the Clipper Chip clearly demonstrated.

Furthermore, key recovery will simply not be widely accepted in the marketplace, even for use on stored data, without having in place privacy safeguards defining how and under what circumstances law enforcement agents and others may get access to decryption keys or decryption assistance. Many users have legitimate concerns about investing in, let alone using, key recovery products without clear answers on how the FBI, or foreign governments—including those with bad human rights records or a history of economic espionage—will get access to their keys. We need clarity on these fundamental privacy issues.

Moreover, costs will be associated with keeping secure the highly confidential decryption keys that a key recovery system will generate. Not every computer user will be able to, or will want to, bear those costs, particularly over long periods of time. How much would such a system increase the cost of using strong encryption? These practical considerations about key recovery systems make compelled or coerced adoption of such schemes entirely inappropriate and downright foolhardy.

NEEDED: STRONG ENCRYPTION

We are mindful of the national security and law enforcement concerns that have dictated the Administration's policy choices on encryption. These agencies fear that the widespread use of strong encryption will undercut their ability to eavesdrop on terrorists or other criminals, or decipher computer files containing material evidence of a crime. But in trying to stuff the encryption genie back into the bottle with policies that threaten privacy, the FBI is short-sighted.

Strong encryption is a significant crime-prevention tool to stop online theft, vandalism and snooping. Just last month, we learned that Defense Department computers had been the target of a aynchronized cyber-attack. The vulnerability of our gov-

ernment computer systems puts vast amounts of sensitive government information at risk of unauthorized access and disclosure.

Government computer systems are not the only ones at risk. Computer security is not just a law enforcement issue; it is also an economic one. Breaches of computer security are resulting in direct financial losses to American companies from the theft of trade secret and proprietary information. This hurts our economy. We should keep in mind the adage that "the best defense is a good offense." Americans and American firms must be encouraged to take preventive measures and use encryption to protect their computer information and systems.

We need to encourage—and not stand in the way of—the use of strong encryption and other technical solutions to protecting our computer systems. Encouraging the use of strong encryption is a plus for both our law enforcement and national security agencies. Strong encryption protects Americans and American businesses from industrial espionage and foreign spying, and strong encryption reduces the vulnerability of electronic information to online snoops and breaches of privacy. Also, importantly, adopting an encryption policy that protects the global competitiveness of our high-tech industries will serve our national security interests better in the long run than driving encryption expertise and markets overseas.

I look forward to working with the Chairman and other Members of this Committee to craft a constructive American encryption policy that gets the government out of the way of better privacy protection for our electronic communications and information. Our national encryption policy has focused almost entirely on the needs of our law enforcement and national security agencies, neglecting the needs of individuals, businesses and our economy. We have a legislative stalemate right now that needs to be resolved, and I hope it can still be resolved in this congressional session. We need to bring some common sense and better balance to this issue.

Senator ASHCROFT. The record will remain open for a week. If anyone chooses or wants to submit something, I would encourage you to do so. I find your analysis very helpful. I think there is a paucity of information and understanding in the Congress about this set of issues, and so I would invite you to supplement your presentations in any way that you feel would be appropriate.

I am hoping that today's hearing will balance the debate on encryption so that the important privacy interests of innocent citizens are not ignored. I am particularly grateful for all your contributions there. I enjoyed Professor Epstein's risk-balancing and risk analysis. It has a certain Chicago flavor about it. However, it has been 30 years since I was at law school in Chicago, and I would have to ask you to slow it down a little bit if I were there today. Maybe it is just that the cranial matter deteriorates with age.

Law enforcement has important and legitimate concerns with encryption, but those concerns must be balanced against the rights of law-abiding citizens, just as they have been in other contexts and other generations. Of particular interest to me has been the focus on the historic involvement of Americans with encryption, and the assumption that somehow we are smarter and more sophisticated than they were a couple hundred years ago. That is an assumption which reveals our ignorance rather than our intelligence. And your contributions in that respect are noted and appreciated.

With that in mind, I adjourn the hearing. Thank you.

[Whereupon, at 12:08 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS AND ANSWERS

RESPONSES OF ROBERT S. LITT TO QUESTIONS FROM SENATOR ASHCROFT

Question 1. If the government forced me to hand over a set of my files to a third party who copied them all, returned the originals, and promised not to hand over the files to the government unless and until agents demonstrated to a magistrate that they had probable cause to analyze the files and that the files were relevant, would the original direction that I hand over the files to a third party pose any Fourth Amendment concerns in your view?

Answer 1. The hypothetical you have described would pose significant constitutional concerns, particularly insofar as it contemplates that the government would be providing a third party access to inspect and distribute your personal and sensitive documents. However, the hypothetical differs in certain important respects from the sort of hypothetical "mandatory" plaintext regime discussed by Principal Associate Deputy Attorney General Robert Litt in his testimony.

The hypothetical question appears to assume several things that would not be true under a well-designed mandatory plaintext recovery regime:

(i) that the government would require citizens themselves to "hand over" their personal files to a third party who would be able to peruse those files himself.

(ii) that the third party could lawfully transmit the files to other, nongovernmental, persons and entities.

(iii) that the third party would be bound solely by his or her own "promise" not to hand over the files to the government unless and until agents demonstrated to a magistrate that they had probable cause to analyze the files and that the files were relevant.

A well-designed mandatory plaintext recovery regime—such as the proposed regimes with which the Department of Justice is familiar—would have the following characteristics:

(i) In a plaintext recovery system or key-recovery system, the trusted third party would not possess any personal files belonging to the owner of an encryption product, but would rather possess a copy of the decryption key to that product, or analogous decryption tools, that would be sufficient to decrypt communications encrypted with such products.

(ii) It would be a crime for the trusted third party to use the key (or analogous decryption tools) to obtain unauthorized access to private citizens' files, communications and data.

(iii) It would be a crime for the trusted third party to transfer the key (or analogous decryption tools) to any unauthorized person, inside or outside of the government.

Accordingly, the third party would not be able to violate the privacy or sanctity of private information, unless that party were willing to expose itself to criminal sanction. The same, of course, is true today: a person willing to expose himself to criminal sanctions can break into your house and steal your personal files. Thus, contrary to the concerns expressed by Professor Sullivan, a well-designed plaintext recovery regime should not "dramatically multiply the opportunities for information to be transferred into the wrong hands through the mistaken or fraudulent release of keys." There would be no appreciable risk of abuse, just as there is not a strong likelihood today that banks will violate their trust and their legal obligations by inspecting the contents of private safe-deposit boxes or revealing such contents to unauthorized persons. What is more, any fear of abuse could be tempered considerably by permitting encryption manufacturers, distributors and/or users to choose among

numerous third parties with whom to entrust their key (or comparable decryption tools).

Importantly, as the Department explained, any legislation in this area, whether or not it imposed plaintext recovery requirements, should not lessen the showing the government must make to obtain access to plaintext from a trusted third party. If a search warrant for data was required before, it should be required under any new regime. We believe that such a regime could be structured to comply with the requirements of the Fourth Amendment. Moreover, Congress could require under such a regime that even if law enforcement obtains a search warrant for data or communications, it would need additional authority, such as a court order, to obtain the key or other information necessary to perform any decryption if the information is encrypted.

Question 2. Some have argued that the mandatory imposition of domestic key recovery is comparable to the mandate in CALEA (Communications Assistance for Law Enforcement Act). CALEA ordered telecommunicationa carriers to ensure that their systems could continue to accommodate wiretaps regardless of the introduction of new technology or services.

(a) Could you tell me your best estimate of the cost of compliance with CALEA? Do you know if anyone has estimated the costs?

Answer 2a. Currently, there does not exist a government estimate of the cost of compliance with CALEA.

The telecommunications industry is in the best position to provide an estimate of the cost to comply with CALEA. Specifically, it is the manufacturers of telecommunications equipment that, to a large extent, will determine the cost of implementation. Carriers will determine the cost of deploying CALEA-compliant solutions. However, to date, manufacturers' concerns over competitive issues and proprietary information have made them either unwilling or unable to provide cost data to the government.

CALEA authorized $500 million to reimburse telecommunications carriers for costs associated with modifying equipment, facilities or services installed or deployed on or before January 1, 1995. The $500 million was not intended to cover all costs of CALEA compliance. Rather, it was to be applied to embedded base equipment, facilities or services within areas of highest law enforcement priority. Equipment, facilities or services of carriers which are not reimbursed will be grandfathered until such time that they undergo significant upgrade, major modification or are replaced. Thereafter, the cost of making equipment, facilities or services CALEA-compliant will be borne by carriers if that action is determined to be reasonably achievable.

Question 2b. How would the administration like to see the use of encryption for telephone communications treated? How would that differ from the current provisions of CALEA?

Answer 2b. The Administration has steadfastly maintained that encryption is extremely beneficial when used to protect the privacy of communications and continues to support the availability and use of such strong, commercially available encryption products and services for legitimate purposes. However, the Administration, and all of law enforcement, is extremely concerned about the serious threat to America's public safety and national security posed by the proliferation and use of strong, commercially available, non-recoverable encryption products and services by criminals and terrorists because such products and services prevent law enforcement from gaining lawful access to plaintext of encrypted, criminally related communications in accordance with the Fourth Amendment. It is for this reason the Administration, and the entire law enforcement community, is calling for the adoption of a balanced public policy concerning commercially available encryption products and services. Such a balanced encryption policy must satisfy both the needs of individual and companies for communications privacy and the nation's public safety and national security needs. Unfortunately, most commercially available products for encrypting communications are non-recoverable and do not allow for access to the plaintext of such lawfully seized, criminally related communications.

In response to continuing advances in telecommunications technologies which were thwarting law enforcement's lawful ability to conduct court ordered electronic surveillance, Congress enacted CALEA for the purpose of clarifying the existing statutory obligation of telecommunications carriers to provide law enforcement with the technical assistance necessary to carry out surveillance under court order or other lawful authorization. CALEA only applies to telecommunications carriers and is not applicable to information service providers, private network and interconnection services and facilities, entities that are nevertheless required by the federal wiretap statute to provide law enforcement with the technical assistance necessary to carry out surveillance under court order or other lawful authorization.

Under Section 103(b)(3) of CALEA, telecommunications carriers are only required to have the ability to decrypt and provide to law enforcement the plaintext of encrypted communications if:

(1) The product or service used to encrypt the communication was provided by the telecommunication carrier, and

(2) The telephone company itself possesses the information necessary to decrypt the encrypted communication.

The Administration believes that public safety and the national security would be better protected if all products or services that encrypt communications include the ability to provide plaintext to law enforcement when legally authorized.

Question 2c. Isn't it true that CALEA requires telephone common carriers to design their systems to preserve what has always been in their control, that is, the isolation and routing of calls so that they can be intercepted by law enforcement? And isn't it true that by contrast the FBI proposal requires manufacturers to take away from users the control over their keys? So, how are these two similar at all?

Answer 2c. Both CALEA and the Administration's encryption policy are concerned with preserving the surveillance abilities that Congress and the Courts have provided to law enforcement in the face of technological change, so to that extent the underlying issues are similar. The particular technical questions they present are, however, somewhat different.

RESPONSES OF ROBERT S. LITT TO QUESTIONS FROM SENATOR LEAHY

Question 1. According to the Vice President's letter of March 4, 1998, the Administration is making efforts to engage in a "dialogue" with industry to "produce cooperative solutions."

(a) If this negotiation effort does not produce satisfactory solutions, will the Administration then consider seeking to legislate domestic controls on encryption?

(b) If this negotiation effort does not produce satisfactory solutions, will the Administration then consider seeking to legislate import controls on encryption?

Answer 1a and b. Although we have no present plans to seek domestic controls, if the negotiations do not produce satisfactory results, the Administration may consider the entire range of legislative options that could implement a policy that balances the need of citizens, business, law enforcement and national security.

Question 1c. Does the Administration support the proposals in the "Technical Assistance Draft" bill circulated by the Federal Bureau of Investigation in August 1997?

Answer 1c. The Administration believes that the "Technical Assistance Draft" bill recognizes the important concerns of protecting the public safety and national security. The Administration has not, however, endorsed the bill and prefers approaches that do not involve mandatory key recovery.

Question 2. Five versions of the SAFE bill, H.R. 695, are currently pending in the House of Representatives. Which version, if any, does the Administration support?

Answer 2. The Administration is not supporting any particular piece of legislation at this time, because we prefer a voluntary, cooperative approach. For some time, the Administration's position has been to encourage the design, manufacture, and use of encryption products and services that allow for the plaintext of encrypted data to be recovered. The Administration is in the process of pursuing an intensive dialogue between industry and law enforcement. Our goal in this process is to bring the creative genius of America's technology leaders to bear in developing technical, market-savvy solutions that will enable Americans to realize the benefits to strong encryption while continuing to protect public safety and national security. The Administration is not advocating any single product, technology, or even technical approach. Rather, we are flexible—provided that the resulting solutions and arrangements preserve the Nation's ability to protect the public safety and defend our national security.

Question 3. While the various agencies within the Administration have expressed concern about the export control provisions in the "Encrypted Communications Privacy Act," S. 376, please identify the concerns, if any, of the Department of Justice with the bill's proposed new sections, §§2801, 2802, 2803, and 2804 of Title 18, which sections provide, *inter alia*, procedures for law enforcement access to decryption keys or decryption assistance?

Answer 3. We believe that timely access to plaintext by law enforcement authorities acting under lawful authority is an important goal to ensure public safety and national security. In light of the Administration effort to work with industry rather than pursuing a legislative solution, we do not believe it is appropriate to comment on particular provisions of specific bills. We think constructive dialogue in a variety

of areas and fora is far preferable to a stalemate that arises from a battle of wills and rhetoric; working together is better than fighting legislative battles.

Question 4. The FBI Director acknowledged in testimony on July 9, 1997 before the Senate Judiciary Committee that while law enforcement is interested in access to encrypted communications there may be little market interest in key recovery for communications. As Director Freeh then stated, "You can't let the market forces deal with this public safety issue because their interests are quite different from ours." Do you agree that while some businesses and users may opt to use key recovery for stored data, there is little interest in the market for key recovery systems for communications?

Answer 4. Although there has been some preliminary interest in recovery systems for communications, there does not appear to be a market for such systems at the present time.

Question 5. Former Senator Sam Nunn testified on March 17, 1998, before another subcommittee of the Judiciary Committee that "the continuing federal government-private sector deadlock over encryption and export policies * * * must be broken and that a consensus must emerge [since] encryption is essential for infrastructure protection * * * [and] if the deadlock continues, building the trust required between the public and private sectors in the broad area of infrastructure protection will be even more difficult." Do you agree that resolution of the encryption debate is crucial for enhancing protection of our country's critical infrastructures?

Answer 5. The Administration believes that resolving the encryption debate is an important priority. Encryption can help protect our national infrastructure, as can products that ensure the recovery of encrypted data. That is why we are engaged in a process of intensive discussions with industry.

Question 6. Former Senator Nunn indicated that the National Security Council should do a better job of coordinating encryption policy among the Federal agencies. Is the Administration taking any steps to address this concern? If so, what steps are being taken?

Answer 6. The Administration is fully satisfied with the National Security Council's efforts on encryption.

Question 7. The Administration is "not wedded to any single technology solution." Please, identify the alternatives to key recovery that the Administration is examining to provide law enforcement with surreptitious access to encrypted communications and data.

Answer 7. The Administration is not advocating any single product, technology, or even technical approach. Rather, we are flexible—provided that the resulting solutions and arrangements preserve the Nation's ability to protect the public safety and defend our national security. Specifically, even if a product is not key recovery, if it provides a means to recover encrypted data or communications it could be satisfactory to the Administration. We hope that our ongoing constructive discussions with industry will permit the flexibility to identify a variety of solutions.

Industry has the technical know-how to develop commercially viable mechanisms that maintain the government's ability to safeguard its citizens, while protecting our citizens from unwarranted intrusions from any source. The primary responsibility for developing technical solutions—be they key recovery solutions or other solutions—lies with industry, which has the expertise and the institutional interest in seeing the success of its products. Just as the computer industry has developed low cost encryption products, we look to industry to develop recovery solutions that can balance commercial and privacy interests and public safety and national security needs.

Question 8. The Administration has sponsored ten pilot projects as part of its "Key Recovery Development Pilot Project" (KRDP).

Question 8a. In September 1997, the National Security Agency advised me in response to written questions that information about the results of the KRDP would "be available in about 60 days." Please provide me with the results of those pilot projects.

Answer 8a. It is anticipated that the final report will be completed in June or July of 1998 and we will provide it to you at that time.

Question 8b. In January 1998, the FBI advised me in response to written questions that "a final market analysis encompassing all the lessons learned, issues, recommendations and market data will be developed" at the conclusion of the KRDP. If that analysis has been completed, please provide it to me. If not, when will it be completed?

Answer 8b. It is anticipated that the final report, which we understand will include the final market analysis, will be completed in June or July of 1998 and we will provide it to you at that time.

Question 9. I understand the entire FORTEZZA Program of Key Recovery with escrowed keys has been discontinued.

Question 9a. If that understanding is correct, please explain why this program was decommissioned?

Answer 9a. The use of the CLIPPER Chip is no longer supported in the FORTEZZA product line. In its place a private key escrow scheme that operates within the high assurance Public Key Infrastructure (PKI) supporting FORTEZZA Cards has been instituted. This scheme is being used to meet the key recovery requirement of the Department of Defense's Defense Messaging System (DMS). In this implementation the Certificate Authority (CA) Workstation when initializing a FORTEZZA Card securely escrowa the private component of the public key pair used for confidentiality. The escrowed private key can be used to support the recovery both of encrypted data that has been stored and encrypted data that is in transit.

The Department of Defense has moved to a Key Recovery concept that would allow corporate and self escrow based implementations. The private key escrow concept adopted for FORTEZZA allowa a distributed architecture for key recovery and allocates the Key Recovery Agent responsibility to the owners and operators of the CA function.

Question 9b. Is the FORTEZZA program with escrowed keys being included in the report or analysis of the KRDP?

Answer 9b. No, there were no KRDP pilots sponsored using FORTEZZA.

Question 9c. Is the Department, the FBI or any other federal agency using telephones with CLIPPER Chips key escrow technology?

Question 9d. How many telephones equipped with CLIPPER Chips are currently being used?

Answer 9c and d. The FBI purchased approximately 9,000 TSD–3600s. It distributed approximately 2,900 TSD–3600s to the Department of Justice, 1,000 to the Drug Enforcement Administration, 1,000 to the United States Marshall Service, and 1,200 to the Department of the Treasury. The Bureau distributed the remaining CLIPPER Chip telephone security devices to its Headquarters, Field Offices and Legats. The Department of Justice and its components do not maintain information on how often the TSD–3600s are used and we do not know the extent to which the Department of the Treasury uses its TSD–3600s.

NSA has informed the Department that it has approximately two dozen telephones that rely on the CLIPPER Chip technology, but that those telephones are not in use. We do not know the extent to which other agencies may use the CLIPPER Chip technology.

Question 9e. If these CLIPPER Chip equipped telephones are not being used, please explain why not?

Answer 9e. The Department has not studied the extent to which its staff use the TSD–3600s or the reasons why they may not be used. We should note, however, that the CLIPPER Chip technology has never been authorized for use in classified communications.

The NSA has informed the Department that it used a small number of CLIPPER Chip devices during the time NSA was assisting the National Manager for Key Escrow and the Escrow Agents in the design, development and deployment of the CLIPPER Chip. NSA reports that it now sees no further use of the CLIPPER Chip concept in communications equipment, the NSA involvement has fallen dormant along with the use of the CLIPPER telephone devices.

Question 9f. Is the government's experience with CLIPPER Chip equipped telephones being included in the report or analysis of the KRDP?

Answer 9f. No, because it was not a pilot of the KRDP.

Question 9g. Are the escrow agents for CLIPPER Chips equipped telephones functioning or whether they have been decommissioned?

Answer 9g. There is still a capability for the CLIPPER escrow agents to retrieve keys. However, it is our observation that to return CLIPPER to an operational status would take considerable time. It is our understanding that all of the Escrow Agent staff at NIST and Treasury has been reassigned; however, the escrow files still exist at these agencies.

Question 10. In January 1998, the FBI advised me in response to a written question that the "Department of Justice is studying the feasibility of utilizing Bilateral and Multilateral Agreement Treaties which are currently in place" for providing foreign governments with keys to the encrypted files and communications of Americans.

Question 10a. Have any of agreements on the provision of decryption keys or decryption assistance been negotiated?

Answer 10a. The Department of Justice is of the view that existing bilateral and multilateral agreements will permit law enforcement assistance as appropriate. This does not mean that law enforcement will routinely share keys with foreign governments. Typically, law enforcement would expect to provide decryption assistance rather than keys in response to foreign law enforcement requests for assistance.

Question 10b. Please identify the concerns, if any, of the Department of Justice with the proposed new § 2806 of Title 18 in S. 376, which section provides standards for release of decryption keys or provision of decryption assistance to foreign governments.

Answer 10b. As mentioned above, in light of the Administration effort to work with industry rather than pursuing a legislative solution, we do not believe it is appropriate to comment on particular provisions of specific bills. However, we would reiterate our view that existing bilateral and multilateral agreements will permit law enforcement assistance as appropriate.

RESPONSES OF KATHLEEN M. SULLIVAN TO QUESTIONS FROM CHAIRMAN ASHCROFT

Question 1. Under the First Amendment, isn't there something of an overbreadth problem with a law that prohibits everyone from using a device with numerous legitimate applications to prevent a few illegitimate uses?

Answer 1. Yes. Total bans on a medium of expression—here, securely encrypted internet communications—are strongly disfavored under First Amendment law. Normally the government is expected to regulate more precisely to target potential problems stemming from speech. A content-based law must be the least speech-restrictive means of targeting a problem. But even if a law is content-neutral, as a law aimed at facilitating law enforcement might well be thought to be, it must be narrowly tailored to its ends. Blunderbuss prohibitions, without any attempt at limitation to particularly dangerous markets or uses, are difficult to describe as narrowly tailored. The problem of overbreadth here is particularly acute when corporations handling massive amounts of information are subject to encryption regulations that fail to distinguish among transactions posing very different levels of risk to government interest.

Question 2. Does the sheer volume of material that may be decrypted on a hard drive compared to the relatively modest scope of a typical telephone wiretap effect the Fourth Amendment analysis?

Answer 2. Yes. The Fourth Amendment, by its terms, imposes an obligation of particularity on the government when it seeks a warrant to search or seize our persons, houses, papera or effects or their modern-day equivalents: warrants shall not issue unless they set forth probable cause "particularly describing the place to be searched, and the persons or things to be seized." The statutory framework we have developed to regulate telephone wiretapping tries to embody the value of particularity by narrowly limiting the scope and duration eavesdropping searches, and by requiring the government to refrain from listening to conversations unrelated to the purpose of the inquiry. Decrypting an entire hard drive to flush out one or a handful of allegedly incriminating communications, in contrast, is more akin to a general search, the very sort of practice against which the Fourth Amendment was originally directed.

Question 3. If the government simply banned encryption technology (or deadbolt locks) would that action raise any Fourth Amendment concerns? How about First Amendment problems?

Answer 3. Yes. Forcing the people to transfer a key to an encrypted document (or to a deadbolt lock) to a third party who for this purpose becomes a federal agent arguably constitutes a search and seizure at the moment it occurs. Making it more difficult for the people to shield themselves against government searches by banning encryption (which of course necessarily makes it more difficult for the people to shield themselves against private marauders as well) may not quite as obviously constitute a literal search or seizure, but it plainly raises serious Fourth Amendment concerns—just as would banning deadbolt locks or non-glassine envelopes. Ordinarily, we are free to protect ourselves from intrusive scrutiny by using commonly available measures; cutting off access to such measures increases the probability that an unreasonable search or seizure will occur by making it more likely that it will succeed. The government might well reply that increasing the potential level of searches should not matter because Fourth Amendment protections still remain for those that do occur, but that ignores the extent to which the lack of protection will decrease privacy at the outset and so change the nature and volume of information that will be produced and stored.

The First Amendment has often been interpreted to raise doubt about laws that predictably decrease the quantity of speech people would otherwise engage in. *Buckley* v. *Valeo*, the case striking down political expenditure limits, for example, reasoned that "the primary effect of these expenditure limitations is to restrict the quantity of campaign speech," an effect sufficient to trigger strict First Amendment review which the limits could not survive. Likewise, a ban on securely encrypted communications would predictably discourage speech, just as would a ban on the use of envelopes to enclose letters sent by mail. Such a disincentive to the full and free exchange of ideas would raise serious First Amendment concern.

RESPONSES OF KATHLEEN M. SULLIVAN TO QUESTIONS FROM SENATOR LEAHY

Question 1. Ms. Sullivan stated that "cooperative solutions may not be constitutional." Does this observation suggest that Congress must closely monitor the results, if any, of the Administration's ongoing negotiations with industry on resolving the encryption debate?

Answer 1. Yes. Neither branch should be eager to countenance "agreements" that are in fact regulatory in nature. For the government to impose conditions on particular transactions in its capacity as trading partner is fine. For the government to require back-door key recovery in all of a private entity's transactions as a condition of doing any business with the government is another matter. The Supreme Court has long suggested that conditions on funding must be "germane" to the purposes of that funding; earmarking federal expenditures for particular uses is unproblematic, but using government leverage to alter what a contractor does in all areas of its business raises difficult, although not entirely settled, constitutional issues. Constitutional concerns such as these may not be waived by agreement, and thus should help to inform both the Administration's negotiations in this area and the Congress's oversight of them.

Question 2. What constitutional problem, if any, would arise if the Administration administratively restricted the importation of encryption with a key length of over 56 bits?

Answer 2. Discrimination against foreign trade is constitutional to the extent Congress authorizes it. Assuming adequate statutory authorization, such a ban would stand or fall with a comparable domestic encryption ban on First and Fourth Amendment grounds.

Question 3. Ms. Sullivan testified that conditioning "the right to make or sell encryption software upon the government's prior approval of that software's key recovery capabilities might raise familiar First Amendment concerns about prior restraint." What constitutional problem, if any, would arise if the government did not require "prior approval" of key recovery capabilities, but instead required manufacturers of encryption software to meet a result-oriented standard that law enforcement be able to obtain immediate access to the plaintext of encrypted information, with violations subject to criminal or civil penalties?

Answer 3. Under the First Amendment, the possible remaining problem with this approach would be that it might diminish incentives to speak (see answer #3 to Senator Ashcroft above) because making such decryption capacity available to government will, of necessity, make it available to private criminal interlopers as well. For Fourth Amendment issues, see #4(b) below.

Question 4. Ms. Sullivan testified that analogizing mandatory key recovery to "the requirement that digital telephones be configured to allow the government to wiretap conversations * * * is inapt" because "[t]elephone users necessarily surrender some control of their communications to telephone companies" and "by contrast, the Internet makes possible unmediated communication between speaker and listener." Just as telephone communications are facilitated by telephone companies, however, Internet communications are facilitated by Internet service providers.

Question 4a. Is the point of this part of the testimony that efforts to regulate user-controlled encryption may trigger different constitutional considerations than regulating service provider facilities?

Answer 4a. The point of this part of the testimony was to suggest that telephone users may be deemed to have partially waived their reasonable expectations of privacy in telephone calls for Fourth Amendment purposes to the extent that they have always been aware, from the dawn of telephones, that the telephone company may be able to intercept those calls. For this reason, the Court has held that there is no Fourth Amendment search or seizure when the telephone company keeps a pen register of numbers dialed—any more than when a bank surrenders copies of one's canceled checks or government agents pick up household trash left curbside where it might also be searched by sanitation workers and scavengers. The issue of what

constitutes a reasonable expectation of privacy has long turned on notions of custom and usage. In a nascent field such as Internet communications, we of course have little in the way of longstanding custom to go by. But to the extent that Internet service providers have to date served merely as disinterested conduits for speech—a status reflected, for example, in Congress's provision in the Communications Decency Act that they should not be understood as publishers for tort purposes—one is entitled to reasonable expectations of privacy against them.

Even if courts analogize ISP's to telephone companies, reasonable expectations of privacy ought extend to the content to messages, as opposed to the addresses accessed. An ISP might log addresses as the telephone company logs phone numbers dialed. But it does not follow that common carriers of either type ought to be presumed able to overhear the calls or messages sent over their lines.

Question 4b. What constitutional problems, if any, would arise if service providers for wire and electronic communications (which includes both telephone companies and Internet service providers) were required, to the extent they provided encryption services, to provide only encryption that enabled law enforcement to obtain immediate access to the plaintext of encrypted communications?

Answer 4b. Under the Fourth Amendment, forcing speakers who are bearers of reasonable expectations of privacy in their encrypted communications to surrender keys to a third party who is in effect a government agent for this purpose arguably amounts to a search and seizure triggering the protections of the Fourth Amendment. This proposal merely shifts the responsibility for search and seizure from the third-party escrow agent to the ISP, who is under government compulsion to open the speaker's communication to government view, and who presumably would not do so if the matter were left to the market. Thus it is not clear how this approach would eliminate any Fourth Amendment objection.

Response of Richard A. Epstein to a Question From Chairman Ashcroft

Question. Do you believe that Congress can insulate the United States from liability for economic losses occasioned by mandatory key recovery despite the Takings Clause?

Answer. The answer comes at several levels. First, as I mentioned in the testimony, it is not clear at present whether the takings clause would hold the United States liable for losses occasioned by the mandatory key recovery system. The taking clause is often focused on matters of physical dispossession, and many cases hold that any alteration of liability rules is within the power of the United States to effectuate. But those cases typically involve reassignments of liability between private parties, and do not concern the direct liability of the government. In these cases, it seems odd that the government can both seize the information and then insulate itself from the losses that follow. But the question is atill open as a matter of current constitutional law.

Assuming that the takings clause does apply, what can the United States do to insulate itself from liability? Here the obvious answer is to make sure that the independent key escrow agent takes that liability upon itself. But that solution is subject to two major defects. First, no independent third party would assume that risk unless compensated for it. And that will require someone to pay. It seems hardly appropriate that private companies should pay to implement programs to which they are opposed, and from which they derive no direct benefit. So the compensation should come from the United States, which now pays, as it were, in advance to have someone else take the risk for it. But that solution is unsatisfactory because once the leak takes place, it will be difficult to trace it to some dereliction by the third party source. The leak could have come from the company itself, or from the government should it take the material. Indeed the liability issues are always difficult when many parties share access to the same information. How the burdens of proof will sort themselves out, and how damages will be measured are anyone's guesses. But I should hope that if the Constitution imposes the obligation on the government to compensate for information that it takes and then loses, that there would be no easy out. After all, there is no easy out that allows the government to escape liability when it takes land for public use. Why have a different result here.

Responses of Richard A. Epstein to Questions From Senator Leahy

Question 5. While Professor Epstein describes as "inappropriate" any government stipulation that "it would not do business with any firm that refuses in its unrelated transactions to adopt a system of escrowed key recovery," would such a stipulation

be unconstitutional? Moreover, would such a stipulation for related transactions be either inappropriate or unconstitutional?

Answer 5. It is quite clear that current Supreme Court law regards the relatedness of the two transactions as key to deciding whether the doctrine of unconstitutional conditions applies. And surely the distinction has some role to play in any overall analysis. Thus if the United States insisted that it have a back door key to any transaction to which it was a party, one would be hard-pressed to say that it abused its state powers by imposing a condition that is found in ordinary business transactions between private parties. So the constitutional pendulum would swing heavily to the government aide. But the situation is quite different if the rule stated is that private firms can only do business with the government if they give the government keys to all their transactions, for now the state is imposing the kind of condition that in all likelihood it could exact only if it had monopoly power. Most private firms would find it impossible to obtain those terms in competitive markets. So here the constitutional doubts would increase. But the issue is not settled today.

As to the appropriateness of the government behavior, a lot depends on collateral circumstances. I could easily see a private company object to the terms on the ground that the loss of information will prejudice its activities not only in this particular transaction with the government, but elsewhere, as with the loss of trade secrets generally. But so long as the one transaction is not tied to others, then it still has the option of forgoing this transaction. If the government cannot find another contractor, then it can rethink its position. But if it can, then it is hard (since there is no tie-in arrangement involved) to attack its decision as inappropriate. It looks instead like a case of hard negotiation between parties who have different interests.

Question 6. What constitutional problems, if any, would arise if the government required that any encryption product manufactured, sold, distributed or imported in the United States be "recovery-capable"—that is, the product must have the capability to be turned on at the purchaser's option to provide access to the plaintext of encrypted information without the knowledge or cooperation of the user?

Answer 6. I do not think that the fact of importation changes the analysis at all. Thus suppose that the United States allows strong encryption for domestically made products. What possible reason is there to impose the limits on encryption on imported products. Even if the ban were perfectly constitutional, no one would buy the products, and the real issue would be discrimination against foreign trade. So now suppose that the ban is imposed on domestic products. If it is unsustainable against fourth amendment objections for domestic products, then it is unsustainable against foreign products. And it would be very odd, if claims are made by users, to say that the ban would be unconstitutional against domestic products but constitutional against imports. The two cases stand and fall together.

RESPONSE OF TIM D. CASEY TO A QUESTION FROM CHAIRMAN ASHCROFT

Question. I understand from your testimony that some may be seeking to require MCI and other on-line service providers to monitor, if it were possible, all electronic traffic that may cross their system. Do you believe that a good encryption policy will solve this problem or do we need more?

Answer. As explained in my testimony before the subcommittee and in other forums, monitoring all electronic communications for the presence of copyright violations or other illegal conduct is not possible as a matter of technology and as a matter of law. Even if the technology were available to monitor the content of communications to the level necessary to perceive a copyright violation, for example, such allocation of human and electronic resources would undermine even the current efficiency of the Internet and certainly would destroy its potential as a future mass medium of commerce and communications.

In addition, as a matter of law, any legislation that would require service providers to monitor the content of all electronic communications would implicate the First, Fourth, and Fifth Amendments of the U.S. Constitution. Another important consideration is the Electronic Communications Privacy Act. Under that law, carriers like MCI are generally prohibited from reading their customers' 3-mails or other electronic communications. As a result, any monitoring requirement would implicate that Act.

Nonetheless, MCI and other service providers understand the concerns of copyright holders in the age of digital communications. As the Chairman is likely aware, the service provider and content communities have recently crafted a compromise that will provide recourse for victims of copyright violations without imposing on service providers the behemoth and illegal task of monitoring all communications.

We expect the result of these negotiations to be presented for consideration before Congress in the near future.

With respect to encryption as a method of preventing copyright infringement, the argument cuts both ways. As I testified, encryption provides a readily-available and inexpensive tool for copyright holders to protect their works. If copyright holders did a better job of protecting their works as distributed or otherwise made available to the public, their piracy concerns would not be as severe. Unfortunately, once a work has been decrypted by a pirate, the present problem resurfaces, but decent encryption would make a pirate's task much more difficult. On the other hand, encryption will be available to those who are determined to violate the law and cover their tracks in the process, thereby making it more difficult for copyright owners to gather evidence of infringement. As a result, encryption is neither the problem nor the solution with respect to on-line copyright infringement. The wide-spread availability of strong encryption, however, is vital to the health and well-being of the Internet for the myriad reasons to which I and others testified before the Subcommittee.

RESPONSES OF TIM D. CASEY TO QUESTIONS FROM SENATOR LEAHY

Question 1. You testified about the use of encryption to protect copyrights. Could you identify and provide the Subcommittee with examples of how encryption has been used to this end?

Answer 1. Probably the most widely used method of protecting intellectual property on the Internet is through the encrypted distribution of software, music and other copyrighted works. Copyright owners can encrypt works that are distributed electronically, as accessible via e-mail, the World Wide Web, or in accordance with other forms of electronic commerce. A wide variety of commercially available products (for use within the U.S.) allow any user to transmit text documents, sound or image files that are inaccessible without first decrypting the file. This method puts the control in the hands of the individual senders and recipients of works. Encryption will increasingly be used by large content distributors to ensure that works are disseminated securely over the Internet. The American Bar Association maintains a website through which encrypted news articles can be downloaded; however, those articles are unreadable to those who have not previously obtained a key to decrypt the file.

MCI uses marketing and training materials in CD ROM form that contain copyrighted images and writings. We encrypt these materials in order to prevent their unauthorized use or copying. For example, it is possible to encrypt an image on a CD ROM in such a way that the image can be viewed on a computer screen, but not printed or copied to the computer user's hard drive. Such protections are freely available for content delivered over the Internet as well.

Question 2. You referred in your testimony to domain names. I have introduced a bill, S. 1727, directing the National Research Council to perform a comprehensive study of the implications for trademark and intellectual property rights holders of the addition of generic top-level domain names and related dispute resolution procedures. Does MCI support this legislation?

Answer 2. MCI supports the idea of a limited study designed to identify the concerns of trademark owners in the domain name context and to raise awareness of issues associated with revamping that system. I would only caution that given the international response to the Administration's Green Paper on the subject, any such effort should be done in a way that will gain acceptance from the international community. As such, the study should (1) be expressly limited in scope; (2) emphasize that it is meant to complement, and not interfere, with the process already underway; and (3) include as part of the discussion assurances that the National Research Council has a history of impartiality and is not a U.S. governing authority.

As an additional consideration, inviting an international organization involved in these issues—such as the World Intellectual Property Organization—to participate in the study could enhance its acceptance abroad.

RESPONSES OF CINDY A. COHN TO QUESTIONS FROM SENATOR ASHCROFT

MCGLASHAN & SARRAIL,
San Mateo, CA, April 7, 1998.

Re: Subcommittee Hearing on "Privacy in the Digital Age: Encryption and Mandatory Access" held March 17, 1998.

Senator JOHN ASHCROFT,
Chairman, Subcommittee on the Constitution, Federalism, and Property Rights, U.S. Senate, Committee on the Judiciary, Washington, DC.

DEAR HONORABLE SENATOR ASHCROFT: I received your facsimile of April 3, 1998, with two additional questions for me arising out of my testimony before the Subcommittee on March 17, 1998. I will attempt to respond to each of your questions in turn.

Question 1. You made reference in your testimony to a Justice Department Office of Legal Counsel opinion discussing some of the First Amendment problems with restrictions on encryption. Could you summarize that opinion?

Answer 1. For your convenience, I have attached copies of the four Office Legal Counsel memorandums and several related letters. The memorandum which is most detailed in its analysis was written in May, 1978, as a memorandum to Dr. Frank Press, Science Advisor to the Preaident. All of the memos concern the previous regulatory scheme under the International Traffic and Arms Regulations (ITAR). However the substance of the current regulations under the Export Administration Act (EAR) is identical for purposes of First Amendment analysis.

In the memo, the Justice Department states that the controls on the export of cryptographic information do reach First Amendment interests, especially in the area of the regulation of technical data. It observes that since the cryptography export regulations create a licensing scheme on protected expression, they constitute a prior restraint. The memorandum then recites the standard First Amendment tests for prior restraint which must be applied, stating:

"It is established that prior restraints on publications are permissible only in extremely narrow circumstances and that the burden on the government of sustaining any such restraint is a heavy one." (Citations omitted)

It continues:

"Even in those limited circumstances in which prior restrains have been deemed constitutionally permissible, they have been circumscribed by specific, narrowly-drawn standards for deciding whether to prohibit disclosure and by substantial procedural protectiona." (Citations omitted)

The memorandum then concludes:

"Even if it is assumed the government's interest in regulating the flow of cryptographic information is sufficient to justify some form of prior review process, *the existing ITAR provisions we think fall short of satisfying the strictures necessary to survive close scrutiny under the First Amendment.* There are at least two fundamental flaws in the regulation as it is now drawn: First, the standards governing the issuance or denial of licenses are not sufficiently precise to guard against arbitrary and inconsistent administrative actions; Second, there is no mechanism established to provide prompt judicial review of State Department decisions barring disclosure." (Emphasis added)

These cases make clear that before any restraint upon protected expression may become final it must be subject to prompt judicial review in a proceeding in which the government will bear the burden of justifying its decisions. The burden of bringing a judicial proceeding cannot be imposed on those desiring export licenses in these circumstances. The ITAR as it is presently written fails to contemplate this requirement.

The additional memoranda on this subject are dated July 5, 1984; July 28, 1981 and July 1, 1981. The letters are dated August 28, 1994; June 20, 1978 and August 29, 1978. All of these OLC documents conclude that there are important First Amendment concerns raised by the regulation of cryptographic information, and most of them, like the May 1, 1978 memorandum, conclude that the ITAR regulations are unconstitutional under the First Amendment.

Question 2. Are there any limits to your software as speech concept? For example, would it raise First Amendment problems for the government to make it a crime to spread programs containing a virus with the requisite intent?

Answer 2. The limits on the concept of software as speech are the same as the limita on any other speech. For example, just because speech is protected by the First Amendment does not mean that we do not properly criminalize speech in the furtherance of a criminal conspiracy, which constitutes defamation, or which vio-

lates a trade secret. The concept of copyright is not affected by the fact that most copyrighted material is also protected by the First Amendment. The First Amendment similarly does not protect someone's right to yell "fire" in a crowded theater, to pass a ransom note or to send a letter bomb. These basic limitations would apply to software as well as other forms of speech.

Accordingly, it should not raise First Amendment problems for the government to make it a crime to spread programs containing a virus with the requisite intent. Further, any other intentional criminal activity which involved the use of computer software could be prosecuted notwithstanding the fact that the software itself was protected expression, just as it could if the crime involved a letter or a conversion.

I hope this responds to your concerns. Given the serious First Amendment and other constitutional difficulties in the regulation of encryption software and related information, we hope that any bill which you will introduce will recognize these Constitutional issues and will expressly provide for the judicial review necessary under the First Amendment in order to ensure that any new law will be properly implemented by the Administration. Without such protections, our experience in litigating this issue leads us to believe that the Administration will attempt to undermine the basic intention of the law, and rely on the lack of judicial review to avoid censure.

If you would like to discuss these matters further, please do not hesitate to contact me. Thank you again for allowing me to address the Subcommittee.

Sincerely,

McGLASHAN & SARRAIL.
Professional Corporation.
CINDY A. COHN.

[The memorandums and letters referred to in response to Question 1 are retained in Committee files.]

ADDITIONAL SUBMISSION FOR THE RECORD

PREPARED STATEMENT BY RICHARD A. EPSTEIN AND KATHLEEN M. SULLIVAN ON BEHALF OF THE AMERICANS FOR COMPUTER PRIVACY

At the close of the Senate Judiciary subcommittee hearings on "Privacy and the Digital Age: Encryption and Mandatory Access," its chairman, Senator Ashcroft, invited all participants to make further comments on the issues raised during the hearings. We wish to accept that invitation to offer some comments on the testimony and statement submitted to the Committee on behalf of the Department of Justice by Robert S. Litt, the Principal Associate Deputy Attorney General.

We find much to agree with in Mr. Litt's statement. We applaud the decision of the Department of Justice not to seek immediate legislation on the question of mandatory access to private encrypted messages. We appreciate the recognition of the Department that important privacy interests must be respected in working out any long-term viable solution. And we agree that cooperative efforts between the Department of Justice and the affected industries and institutions could improve the harmonization of privacy and security interests. Nonetheless we think Mr. Litt's prepared statement and oral testimony do not do an adequate job in balancing the relevant interests, both on practical and constitutional grounds. Our joint comments express our concerns with the positions taken by the Department of Justice.

Practical and Administrative Concerns. As a practical matter, we think that reconciling the claims of privacy and security pose a more daunting challenge than Mr. Litt acknowledges. He writes: "The Administration's approach [to escrowed key recovery] has found support in the marketplace, in part because businesses and individuals need a routinely available method to recover encrypted information." (Testimony, page 2). This assertion, however, glosses over the very different objectives and requirements of private and law enforcement key recovery. First, private parties have no need or desire for key recovery systems that operate without their knowledge and cooperation; yet that feature is one on which the Department of Justice insists. Second, private key recovery systems do not have to operate within the strict time limits, often measured in hours, that the government demands for its key recovery. Third, a private encryption system does not require the long-term storage of all communications once they are completed, which is one of the central demands of the government system. Fourth, private key recovery does not contemplate the sharing of keys with foreign governments, which is again part of the Department of Justice's present demand.

The cumulative impact of these differences matters. The Ad Hoc Group of Cryptographers and Computer Sciences concluded that "the requirements of government key recovery are almost completely incompatible with those of commercial encryption users." (Ad Hoc Group, The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption, at 7). Nothing in Mr. Litt's written or oral statements explained how these profound differences are to be overcome, or how the widely different private approaches to key recovery could be meshed with a single government imperative. His observation of "marketplace support" may reflect the business decision of a few companies to seek to gain a leg up in the encryption business by complying with the government demands on the use of encryption in export markets. It does not reflect the strong conviction of the many supplies and users of encryption services who remain deeply troubled by the inherent insecurities that mandatory government access introduces into all encryption systems.

Second, we disagree with the Department of Justice's assessment of the ability of private industry to serve two masters by developing secure methods of mandatory access. Mr. Litt observes that industry wizards can always develop "market savvy" solutions to key recovery because of their "technical know-how" to deal with complex problems. But private industry is not able to perform miracles. Once it understands that trapdoor key recovery necessarily compromise the integrity of any encryption device, it can no more design around that problem than a skilled mathematician can

square the circle or reduce pi to a simple fraction. And even if private industry could design the impossible, it could not administer it consistent with the level of security that it demands. Any successful key recovery program requires the extensive cooperation of government agencies, none of whom have in place the massive technical infrastructure that is necessary to manage billions of keys to the massive and ever-expanding stream of encrypted data that is sent over the wires. Yet we have heard nothing to suggest that government has made the huge staffing and resource commitments without which any full-scale program of key recovery will quickly fail; nor is there any recognition that the government or its designated key-recovery agents might have to bear some financial liability when encrypted messages are compromised. The Department of Justice is worried about the possibility that it will be faulted if it does not foil some major terrorist incident without a key recovery system in place. It fails, however, to express equal concern at the possibility that the defective design or ineffective government administration of a mandatory access system could bring on the very catastrophe that it wishes to prevent.

Third, we believe that the Department of Justice has refused to acknowledge the major shortcomings in its surveillance system that will remain even if a comprehensive (but flawed) key recovery system could be put into place. The presence of this system will induce terrorist and criminal elements to find ways to transmit their information outside the system, and to use any of the hundreds of strong encryption devices that are now on the market, both in the United States and elsewhere. Even if constrained to use back door encryption systems, they could flood the system with thousands of false messages to throw law enforcement systems off the scent; they could use multiple layers of code so that the plaintext message recovered is unintelligible to outsiders without further information; and they could always treat the key escrow program as an object of its own attacks. We fear therefore that terrorist and criminal elements will be adept at evading or invading a system that can effectively compromise the legitimate activities or ordinary individuals and businesses. Yet nothing in Mr. Litt's testimony offers reason to believe that trap door recovery will secure the ends of law enforcement against these dangers. What reason is there to believe that drug kingpins will store their "little black books" in a key recovery system when so many unbreakable systems are already freely available in the marketplace?

Constitutional Concerns. Our uneasiness about the practical soundness of the Justice Department's position carries over the analysis of its legal position. Initially Mr. Litt's statement notes that the government is now pursuing "voluntary" cooperation with its programs. To the extent that this expression only means that the government has asked private software manufacturers to include back door keys in their encryption devices, we see no constitutional difficulties with this program—as long as the private manufacturers are allowed to "just say no." But the question of whether the government approach should be regarded as "voluntary" takes on a different coloration if the price for noncompliance with the government position is the loss of government contracts or grants, and when compliance with these government requests promises favorable treatment in a wide range of government programs. And we are even more worried about government requests that strong encryption be used not only in business with the government, but in all business that government contractors and grantees have with other parties. At this point the massive power that government has over all aspects of our economy gives its voluntary requests a far more ominous tone that could easily verge on institutional coercion. An additional concern raised by the Justice Department's position is the prospect of uneven treatment of private and public entities, for we have no doubt that many government agencies (the military, the NSA, Social Security and Medicare operations) would refuse to turn over to the Department of Justice trapdoor keys for their sensitive information.

Our concerns are not eased when we look at some of the constitutional claims advanced in Mr. Litt's testimony. Initially, we take issue with his optimistic assessment that no Fourth Amendment concern is warranted because "a well-designed plaintext recovery regime would ensure that users' reasonable expectations of privacy were preserved." In our view, the relevant set of reasonable expectations should not be shaped by private capitulation to government's insistence on intrusive systems of surveillance. Rather, the original purpose of the reasonable expectations test was to augment private protection against trespassory invasions by requiring government additionally to respect the privacy of ordinary individuals who had made reasonable efforts to keep their information away from the prying eyes and ears of the government and other private parties. That is what the ordinary user of the telephone does by shutting the door to the booth; and that is what private individuals and businesses do when they encrypt their information for storage or transmission. Government may not bootstrap itself out of societal understandings

that some areas of life deserve presumptive protection from government invasion simply by invading those areas. So long as internet users and businesses reasonably believe that backdoor entry degrades the protection that is afforded by strong encryption—just as reasonable expectations of privacy would be degraded if they had to store extra keys to their houses or duplicates of their private papers with government-designated third parties—they are entitled to the traditional protections provided by the Fourth Amendment against unreasonable searches and seizures.

Mr. Litt further claims that private individuals and firms need have no fear of the key recovery system because the government will be able to turn the key in the lock only after it complies with all the requirements that it now faces to getting information, including, where appropriate, any needed search warrants. But the Department of Justice assurance is not responsive to the full set of risks introduced by mandatory government access. It does nothing to address the risks of unauthorized third parties gaining illicit access to confidential communications or dats, or of some rogue law enforcement agents, unimpeded by any notice and knock conditions, conducting unauthorized searches of their own. Nor does it address the invasion of reasonable expectationa worked by the mandatory surrender of privacy at the outset.

Most important, in his oral testimony, Mr. Litt conceded that forcing individuals to turn over their keys to a government-designated agent represents a seizure of that key, thus implicating the Fourth Amendment. If so, then we are baffled as to how he can defend the constitutionality of the system. General warrants and dragnet searches were the prime targets of the Fourth Amendment; they are not insulated from review when the government outsources its activities to chosen contractors who become for these purposes federal agents. The all-inclusive scope of the government-mandated seizure involved in mandatory key access necessarily runs afoul of the Fourth Amendment's requirement that all searches be done only with probable cause on particular description of the items to be seized.

Mr. Litt's ststements also fail to quell our uneasiness about the government's poaition on the potential violation of the Fifth Amendment's privilege against self-incrimination. In his written statement, Mr. Litt suggests that there is no compulsion on a user of encryption if the government merely requires the manufacturer to build in a government-accessible key, ignoring the fact that any compulsion on the manufacturer will run also against the user through the purchase. Mr. Litt also suggests that even compelling the encryption user directly to supply a key to a third party ia unproblematic because such a communication is no more testimonial than a compelled consent form authorizing a foreign bank to disclose bank records, such as the one the Court held permissible in *Doe* v. *United States,* 487 U.S. 201 (1998). This argument ignores important differences between compelled key access and the forced bank record access upheld in *Doe.* First, many communications encrypted on the internet will be private or personal, intended only for the unmediated view of the intended recipient, unlike bank records whose privacy one has waived by voluntarily surrendering information to the bank, see *United States* v. *Miller,* 425 U.S. 435 (1976). Second, the act of producing the key to any particular internet message is arguably more "testimonial" than generic authorization of access to unspecified and thus "hypothetical" bank accounts that was upheld in *Doe.* Finally, even if Mr. Litt were correct that any Fifth Amendment privilege claim against mandatory key access would ultimately fail as a technical matter because the compulsion on the user would be disaggregate from any incriminating testimony extracted from the third-party recovery agent, it is surely constitutionally troubling to design a system for the very purpose of making it impossible for any encryption user ever to assert a Fifth Amendment privilege with respect to an encrypted communication.

Mr. Litt similarly dismisses too readily, we think, important First Amendment concerns raised by mandatory key access. He suggests that encrypted communications do not count as speech at all because numeric code cannot be readily underatood by lay observers. The First Amendment, however, has long been interpreted to protect complex scientific, artistic, musical, or mathematical notation as well as other forms of expression. As the Supreme Court recently noted, "a narrow, succinctly articuilable message is not a condition of constitutional protection, which if confined to expressions conveying a 'particularized message,' would never reach the unquestionably shielded painting of Jackson Pollock, music of Arnold Schonberg, or Jabberwocky verse of Lewis Carroll." *Hurley* v. *Irish-American Gay Group of Boston,* 115 S. Ct. 2338 (1995).

Mr. Litt further suggests that, even if encryption does count as speech, any mandatory key access scheme would merely be required to satisfy the intermediate scrutiny appropriate to "time, place or manner" regulations or "incidental restrictions on communicative conduct." This is far from clear. For one thing, a total ban on a uniquely valuable medium of expression—here, the medium of securely encrypted

internet communications—has never been considered a mere "manner" regulation. A manner regulation merely forces a speaker to shift to a substitute form of communication, but by definition an insecure communication cannot substitute for a secure one. A ban on unescrowed encryption thus resembles the total bans on sign-posting or leafleting that have been struck down as exceeding the limits of permissible manner regulation. For another, Mr. Litt ignores the compulsion of speech entailed by mandatory key access: a third-party must be given information the speaker otherwise would not disclose, and indeed under some versions of key access, that information would have to be textually embedded in each discrete communication the speaker chose to make. But the right to speak has long been thought to entail a strong presumptive right not to speak, including the right to speak anonymously. While compelled speech is permitted under certain circumstances, such as in food and drug labeling or securities exchange disclosures, compelling all users of the internet to disclose their keys at all times and for all purposes would involve compelled speech on an unprecedented and constitutionally troubling scale.

Morever, even if encryption regulation were considered content-neutral, as Mr. Litt suggests it should be, that would not eliminate all First Amendment concern. To the contrary, laws that significantly deter speech may well violate the First Amendment even if they do not prevent the speech altogether, as illustrated by numerous decisions invalidating laws restricting the receipt of payment for speech. It could hardly be argued that requiring letters to be posted in transparent glassine envelopes would be a permissable end run around the unconstitutionality of a fan on the sending of letters themselves.

Most troubling of all of Mr. Litt's First Amendment arguments is his suggestion that mandatory key access will not "chill" speech because it gives government "no greater access to the content of private parties" communications than it currently has." This argument suffers from the same fallacy as his argument under the heading of the Fourth Amendment that forced key disclosure to government-designated agents does not breach reasonable expectations of privacy. In either form, the argument assumes that a government unconstrained by knock-and-announce rules will never err or overreach in seeking keys, and that criminal interlopers will never take advantage of the expanded opportunities for theft or fraud opened up to them by the expansion of non-user-controlled key storage sites. If either assumption is relaxed, as in an imperfect world they must be, then there can be no question of a chilling effect on speech.

Finally, we think that one common thread explains why the Department of Justice has failed to attach adequate weight to the constitutional objections against its proposal. At the end of his testimony, Mr. Litt notes a conversation that he had with a representative of the computer industry who challenged him with this observation: "We don't ban cars, do we? Then why are you trying to ban encryption?" Mr. Litt answered that challenge in two ways. First, he denied that the government seeks an outright ban, but he could not deny that the government proposals if adopted would operate to reduce the levels of private encryption and the security of any encryption still undertaken. Next Mr. Litt sought to justify the proposed government restrictions by enumerating the various types of regulation routinely allowed for automobiles: safety inspections, minimum gas mileage requirements; pollution emission requirements; seatbelts and airbags; drivers' licenses and highway regulations. In his view, the same principles that allow extensive regulation of the automobile allow the proposed regulation of communication.

We believe that his analogy is fundamentally flawed because it overlooks the difference in level of scrutiny brought to different activities. The driving of an automobile, however important it may be in the lives of ordinary individuals, does not implicate the preferred freedom that the Bill of Rights accords to speech. Nor does driving a car on a public highway implicate Fourth Amendment liberties to the same extent as other activities conducted out of public view. The security of the person or of a person's papers against government searches and seizures has long been accorded far more protection that the security of a driver of a car. Hence the scrutiny brought to the use of automobiles is often that of the rational basis test, a deferential standard under which the government is able to prevail by a showing of any reasonable connection between the regulations imposed and the public interest advanced. Indeed most of the regulations listed by Mr. Litt satisfy even greater amounts of scrutiny. Safety inspections and pollution controls help prevent tortious wrongs to other individuals; licensing requirements, speed limits and other safety rules protect each individual user of the highway from harms by others; airbags and seatbelts are also directed at fundamental safety concerns. And the most dubious item on his list, mandatory mileage controls, would at most require the computer and communications industry to increase output and reduce price, which they have done at a dizzying pace.

None of these highway safety regulations begins to touch the interests of individual privacy that lie at the core of the present dispute. Mr. Litt would be hard pressed to show that the government could make comprehensive searches of all automobiles on public highways on the suspicion that some tiny fraction of vehicles might be carrying drugs or contraband—a form of dragnet far more extensive than the limited border checkpoints and temporary roadblocks for sobriety checks that have previously been approved under the Fourth Amendment. Nor could government constitutionally make it a condition of traveling the public highways that all drivers file in advance a copy of their travel plans with a government-designated agent in order to facilitate the government's possible location of a handful of wheelborne criminal suspects. Indeed the most that the government could glean from these highway cases is the possible authority to tag encrypted messages with license numbers so that they could be identified by source. Yet even here the First Amendment's protection of anonymous speech and its prohibition against compelled speech might well be held to strike down those tracing efforts.

The issues raised by this hearing, however, go beyond these legal refinements. The Constitution today affords a high level of protection to privacy interests, which is implicitly denied by the government effort to analogize its mandatory access system to comprehensive regulation of the use of automobiles. Cars represent an area where the case for state regulation is at its peak. Mandatory access to private information represents that are where the government's claims meet with far stiffer resistance. We think it only appropriate to express our grave misgivings with a Department of Justice position that supports regulation of private speech and communication that is more intensive and more intrusive than any scheme of automobile regulation now on the books. Its position represents a manifest inversion of constitutional priorities. Areas of great constitutional sensitivity deserve the highest levels of constitutional protection.

○