CENTER FOR DEMOCRACY and TECHNOLOGY

Testimony of

Jerry Berman, Executive Director
Center for Democracy and Technology
on
How Current U.S. Encryption Policy Fails to Meet the Needs of American Internet Users

Before the
Senate Committee on Commerce, Science and Transportation
Subcommittee on Science, Technology, and Space

June 26, 1996

How Current U.S. Encryption Policy Fails to Meet the Needs of American Internet Users

I. Introduction and Overview

Good morning, my name is Jerry Berman, Executive Director of the Center for Democracy and Technology (CDT). The Center is pleased to have this opportunity to testify today. CDT is an independent, non-profit public interest policy organization in Washington, D.C. The Center's mission is to develop and implement public policies to protect and advance individual liberties and democratic values in new digital communications media. The Center achieves its goals through policy development, public education, and coalition building. CDT also coordinates the Digital Privacy and Security Working Group (DPSWG), an ad hoc coalition of more than 50 computer, communications, associations, and public interest organizations working on communications privacy issues. In the past, CDT and members of the Working Group have strongly opposed the Administration's Clipper Chip proposals.

A. Overview: Encryption Policy in the Internet Age

With the recent Federal court ruling in Philadelphia enjoining the Communications Decency Act, the remaining major legal obstacle to the development of electronic commerce is outdated U.S. encryption policies. The Administration's cryptography policy, based upon a narrow national security perspective that ignores the privacy needs of individual users, cannot form the sound basis for a secure communications infrastructure. A cryptography policy without explicit privacy protections will never gain the trust of users or be embraced by the international marketplace.

In the two years since the Senate last held hearings on encryption policy, the looming crisis in privacy and security has become more urgent, yet remains unresolved:

1. **The Internet Perspective** -- U.S. encryption policy has failed to account for the emergence of the Internet as a model for communications:
    - **The Internet is not like the telephone system** -- The Internet encompasses a range of social functions far beyond simple two-way

voice communication. These broad activities demand a heightened capacity for users to protect their security and privacy online. The traditional approach to wiretapping cannot simply be exported to this new medium.

- **The Internet is a global, decentralized medium** -- Efforts to impose unilateral national policies -- such as export controls or key escrow proposals -- are unlikely to be accepted widely. Decentralized user choice solutions to privacy problems are preferable to and more effective than centralized government mandates.

- **On the Internet, the Bill of Rights is a local ordinance** -- Constitutional guarantees offer no protection to U.S. citizens whose communications regularly cross national borders. Policies should be designed to protect Americans outside of the shelter of U.S. law.

2. **Current encryption policy fails to meet users' needs** -- Widely available strong encryption is essential if users are to ever trust their private and sensitive information to the Global Information Infrastructure (GII). Yet export controls and other policies have kept good encryption tools out of the hands of everyday users and capped security at a 40-bit key length that many experts judge to be "inadequate protection."[1]

3. **Administration encryption policy remains hostage to a law enforcement and national security rationale that is outdated and unsubstantiated** -- National security arguments have been undermined by the increasing availability of strong encryption outside of the United States. The law enforcement problem posed by encryption is real, but narrowly focused around real-time surveillance of electronic communications. The massive invasions of privacy and the high cost of the Administration's export controls and key escrow policies cannot be justified on these narrow and eroding grounds.

Congressional action is needed. Encryption policy is the weak link creating a crisis in electronic commerce and individual privacy. Only Congress is in a position to demand that law enforcement justify its policies. Only Congress can act quickly to reverse the policies of the Administration. CDT strongly commends those of you who have supported S.1726, the Protecting Commerce Online in the Digital Era (PRO-Code) Act of 1996, authored by Senator Burns, and S.1587, the Encrypted Communications Privacy Act of 1996, authored by Senator Leahy. The Congress should act to immediately liberalize export controls and provide American Internet users with the strong security and privacy they so badly need.

B. Internet User Involvement is Crucial

CDT is pleased to be here as part of these important Congressional efforts to address the crisis that exists today in U.S. encryption policy. The Center wishes to express its thanks to you, Mr. Chairman, to Senator Pressler, Senator Wyden, and the other sponsors of S.1726 for your work in support of Internet privacy and security, and to Senator Leahy, who has been a long-time supporter of efforts to ease encryption controls.

We are particularly concerned that the voice of Internet users be heard in this forum. We are pleased to have been a part of the Committee's efforts to solicit input from everyday computer users for this hearing, via the World Wide Web. We are also pleased to be working with HotWired and Digex to make this the first Senate hearing ever simulcast live over the Internet -- making these proceedings accessible to millions worldwide. We commend the Committee for reaching out to the growing community of computer users who care deeply about this issue.

II. Communications Privacy in the Age of the Internet: Public Policy Principles

For years encryption policy has been driven, substantially unchallenged, by the needs of the national security establishment. With the arrival of the personal computer and the Internet, that narrow focus is plainly no longer acceptable. The policies that may have been appropriate for the Age of the Mainframe Computer will not meet the needs of individuals and society in the Age of the Internet. We suggest that any policy that addresses privacy and security on the Internet should do so in light of the following policy principles:

- The Internet is not like the telephone system.
- The Internet is a global medium: Decentralized user choices are preferable to centralized government mandates.
- On the Internet, the Bill of Rights is a local ordinance.[2]

Application of these principles to today's encryption policy logjam leads to the inescapable conclusion that fundamental change is needed. S.1726 has CDT's full support for its effort to move this policy debate beyond the Cold War-era Mainframe model, into the Age of the Internet.

A. The Internet Is Not Like The Telephone System

"The Internet is therefore a unique and wholly new medium of worldwide human communication." Court's Findings of Fact, ¶81, ALA v. Dept. of Justice[3]

If there is one truth that policymakers have learned about the Internet in the last year, it is that the Internet is not just another telephone system. Current encryption policy is justified, in part, by law enforcement arguments that they must continue to conduct electronic surveillance in the same manner as they are able to on the telephone network. But efforts to simplisticly apply assumptions about wiretapping from the telephone system to the Internet risk grave threats to individual privacy. In a similar vein, congressional attempts in the Communications Decency Act to impose content-based restrictions on speech from the phone system onto the Internet have recently been harshly rebuffed by the Federal courts.[4]

From a constitutional privacy perspective, the single most significant difference between the Internet and traditional telephone service is the vast array of uses that the Internet currently serves, as well the even larger range of new applications bound to come in the future. The Internet is not simply a new-fangled digital telephone. Rather, Internet services will likely facilitate the following important social functions now or in the near future:

- wallet
- first class mail envelope
- carrier of credit card transaction
- face-to-face contact with a bank or a merchant
- public library
- neighborhood bookstore
- movie theater
- doctor's office
- town square, coffee shop, union hall, political clubhouse, or community center where we discuss politics
- local art museum
- romantic night spot for intimate conversations

The Internet is much more than simply a means of instantaneous communications like telephone conversations, which are short and largely support other activities that transpire in the physical world. Instead, the Internet is itself a platform where all of the activities listed above can take place. On the Internet, people do business, engage in politics, conduct intimately private interactions with health care professionals, participate in culture, and even fall in love. The vast breadth of activities conducted online demand that individuals have the greatest ability possible to protect their privacy and ensure their security. These activities also demand greater protection against government intrusions on individual privacy, free expression, and freedom of association.

The privacy protections embodied in the U.S. law today are the product of a long and thorough debate in which the concerns of law enforcement were aired and carefully weighed against the rights of citizens. Congress should not allow law enforcement concerns to unravel this delicate balance by imposing the wiretapping paradigm on this new medium without careful deliberation.

Case Study: Application of wiretapping to the virtual corporation challenges Fourth Amendment principles

Wiretapping and other electronic surveillance has always been recognized as an exception to the fundamental Fourth Amendment prohibition against secret searches. Even with a valid search warrant, law enforcement agents must "knock and announce" their intent to search a premises before proceeding. Failure to do so violates the Fourth Amendment. Until now, the law of search and seizure has made a sharp distinction between, on the one hand, seizures of papers and other items in a person's physical possession, and on the other hand, wiretapping of communications. Seizure of papers or personal effects must be conducted with the owner's knowledge, upon presentation of a search warrant. Only in the exceptional case of wiretapping -- and with the heightened procedural and substantive requirements that accompany a wiretap request -- may a person's privacy be invaded by law enforcement without simultaneously informing that person.

In the era where people work for "virtual corporations" and conduct personal and political lives in "cyberspace," the distinction between communication of information and storage of information is increasingly vague. The organization in which one works may constitute a single virtual space, but be physically dispersed. The papers and files of the organization or individual may be moved within the organization by means of telecommunications technology. Instantaneous access to encryption keys, without prior notice to the communicating parties, thus present a much broader intrusion. Such access may well constitute a secret search, if the target is a virtual corporation or an individual whose "papers" are physically dispersed.

B. The Internet Is A Global Medium: Decentralized User Solutions Are Preferable To Centralized Government Mandates

On of the Internet's great strengths is the ease with which it spans the globe: information flows as effortlessly from New York to Nairobi as from Washington, DC to West Virginia. Moreover, a communication from New York to Nairobi might travel

through the United Kingdom and four countries one day, but through France and five other countries the next day. For this reason, national controls are unlikely to work in a global medium like the Internet. Privacy solutions should not rely on centralized policies and control, but instead should be oriented towards the user and robust enough to exist in the highly decentralized environment that characterizes the Internet.

The rapid pace of Internet development has occurred with some important government support, but entirely without the interference of the traditional regulatory process. The flexibility of the Internet community in developing new solutions to meet user needs has been nothing short of astonishing. Yet the one area in which the innovative energy of the Internet has been most stifled has been in the area of security and privacy. Just as we cannot expect the United States government to have anticipated the architecture of the World Wide Web, so it is foolhardy to expect that the national security establishment of the United States can anticipate and provide for the security needs of all Internet users. S.1726 properly gets the government out of the business of controlling this vital part of the emerging information infrastructure.

C. On the Internet, the Bill of Rights is a Local Ordinance

Both data security solutions against private intrusion and privacy protections against unwarranted government surveillance must be suited to the global nature of the Net. Good data security demands strong encryption to foil threats wherever they are in the world. And good data security and privacy policies must recognize that the Bill of Rights in the United States Constitution is nothing more than a local law.

United States Constitutional protections against unreasonable search and seizure offer little protection to U.S. citizens whose Internet communications regularly cross borders. Foreign governments and others can intercept these messages without the knowledge of the senders, and beyond the ability of the United States government to protect the privacy rights of its citizens. For similar reasons, the key escrow agents called for in recent Administration policy proposals would create an enormous new vulnerability for Internet users -- both from private data intruders and from governments which may not have adequate law enforcement safeguards or may not accord the same privacy protections to United States citizens.

The global nature of the Internet thus demands that users have access to the highest quality encryption technology. We strongly agree with the many individuals, fellow privacy advocates, and industry leaders who praise S.1726's effort to lift export controls and allow the market to provide the security and privacy that global Internet users need.

III. The Need for Locks and Keys on the GII: Users Need Encryption

"On balance, the advantages of more widespread use of cryptography outweigh the disadvantages."[5]

The use of encryption is an inevitable and essential part of life online. As the National Research Council found in its long-awaited encryption White Paper, not only do users need encryption, but it is actually in America's national interest to promote the widespread use of good cryptography.[6]

A secure, private, and trusted Global Information Infrastructure (GII) is essential to promote economic growth and meet the needs of Information Age society. Developing that secure and trusted GII requires strong, flexible, widely-available cryptography. Individuals need to have confidence in the GII to realize the full democratic potential of free association and personal communications. Competitive businesses need to protect proprietary information as it flows across insecure global communications networks.

In recent months the public has been made increasingly aware of the dangers of computer crime and the vulnerability of current cryptography implementations. Rapid advances in the speed and sophistication of hardware and software have laid siege to the 40-bit key systems currently approved for export, as well as the popular 56-bit DES algorithm.[7] If we are to maintain the trust of the public and realize the full potential of the GII, individual users will need widely available good encryption to protect themselves online:

- Individuals need encryption in order to trust the GII with confidential data such as financial transactions, medical records, or private communications.

- Businesses need encryption to provide individuals with privacy protection and to protect proprietary information as it flows across vulnerable global networks. Moreover, businesses need good encryption to protect the growing stores of personal information that they accumulate about individuals -- such as medical, insurance, credit, or financial records.[8]

- Government users need encryption. Government itself needs good encryption to protect sensitive military, law enforcement, financial, or private citizen information.[9]

- America needs encryption to promote national security and prevent crime. The widespread use of strong encryption is widely considered one of our best

> defenses in the battle to protect America's information infrastructure from information warfare and other security threats. It is ironic that the very players within the Administration who should be promoting the use of encryption to promote national security and prevent crime online are actively working to stop it. FBI Director Louis Freeh testified in the Senate this Spring about the massive losses attributed to industrial espionage in this country, estimated in the hundreds of billions of dollars. CIA Director John Deutch has testified just yesterday about the increasing vulnerability of our financial, utility, government, and telecommunications information infrastructure to "information terrorists" and other bad actors. Yet the lack of strong encryption use today has left computer users vulnerable to the prying eyes of hackers, corporate competitors, and even foreign governments.[10]

The GII will not fully develop without widely available and strong cryptography. The lack of any international standard for strong cryptography has already hindered the deployment of highly secure systems worldwide. Moreover, national and regional governments are increasingly considering regulations on the use of encryption. Such actions threaten to create a patchwork of international regulations which would hinder the deployment of secure global communications and leave users without the security and privacy they need.

In this context, the sole focus on national security needs embodied in the Administration's cryptography policies is unlikely to meet the needs of GII users. By maintaining 40-bit key length restrictions on exports, these policies leaves users hamstrung with insecure systems. By proposing unattractive interoperability restrictions and minimal privacy protections for key escrow systems, these policies discourage the deployment of secure systems in U.S. products. Rather than being seamlessly incorporated into popular products, secure communications will remain out of reach for less sophisticated GII users. The resulting loss of security will have a chilling effect on the development of electronic commerce and the information infrastructure as the privacy and security needs of users are not met.

IV. "Naked To Mine Enemy"[11] -- The Failure of Administration Encryption Policy: Users' Needs Go Unmet

"Current national policy is not adequate to support the information security requirements of an information society."[12]

Current Administration encryption policy has failed to meet the needs of computer users. Export controls and other government policies keep good encryption out of the

hands of users. These policies act to coerce the domestic market for encryption. The 40-bit key length encryption available under these policies is widely viewed by experts as inadequate. Worse, the export controls are intrusive and ineffective at meeting their stated national security goals. U.S. encryption policy is in a state of crisis, with users unable to get the privacy because of unsupportable national security and law enforcement rationale. Moreover, the Administration's Clipper Chip and subsequent policy proposals have barely acknowledged privacy concerns in any meaningful way, and have been greeted with distaste and scorn by the marketplace and the public.

Current Administration policy restricts the export of "strong" encryption hardware or software products with keys greater than 40 bits long (the length of the "keys" indicates the security of a system). Many experts believe that 40 bit security is woefully inadequate.[13] Export controls actually keep domestic users from getting good encryption. Most U.S. software and hardware companies have been held hostage as they try to make their domestic products interoperable with and subject to the same restrictions as their exportable products. **The result is a government policy that hurts American businesses and individuals:**

- **It hurts individuals** by not allowing them to choose the encryption systems that best meet their security needs. A recent study by a panel of renowned cryptographers found that the systems currently exportable under government policies "offer virtually no protection from brute-force attacks."[14]

- **It hurts U.S. industry** by not allowing companies to provide secure products in the face of strong foreign competitors who are not restricted by export controls. A recent report by the CEOs of 13 large American technology companies concluded that the American computer industry could lose up to $60 billion annually by the year 2000 due to these export controls.[15]

- **It doesn't even meet the needs of national security.** The Software Publishers Association has documented hundreds of foreign encryption products already widely available abroad. Criminals, terrorists, and foreign governments will always have access to good encryption; it is law-abiding citizens who sacrifice their privacy under current law.

Recent Administration proposals would only allow the export of moderately stronger encryption, and then only with "key escrow" restrictions to guarantee U.S. government access to individuals' keys -- restrictions which are bound to fail in the competitive international marketplace.

V. Putting the Administration's Arguments in a Box: Law Enforcement Has Not Made It's Case

Law enforcement has been unable to justify massive losses of privacy it proposes in return for minor gains in surveillance capabilities. The law enforcement problem posed by encryption is real, but narrowly focused around real-time surveillance of electronic communications. The massive invasion of privacy and high cost of the Administration export controls and key escrow cannot be justified by the law enforcement's last, hopeless grasp to expand their capabilities is an area where those capabilities are already largely gone.

Law enforcement faces a real, but narrowly focused, problem with encryption. The vast majority of encrypted information will be accessible to law enforcement by legal process. Stored information, corporate and business information, and even much electronic communication will be largely available to law enforcement through similar legal process available today (See Figure 1 below):

1. Stored business information -- Stored corporate records and business information, encrypted for security and privacy purposes, represents a large part of the use of encryption and will be almost completely accessible to law enforcement using the same sorts of court orders, warrants, and even subpoena processes that are available today to access similar unencrypted data.

2. Stored information by individuals -- Will be similarly available by legal process, just as it is today. In certain narrow circumstances, access to encrypted information may be thwarted by assertion of a Fifth Amendment privilege against self-incrimination.

3. Business communications -- Business communications will be largely accessible to law enforcement. Today, electronic communications almost always become stored information at one end or the other, and often both, and often as plaintext. (For example, consider the instructive example of the archived email in the Bush Administration). Such stored information will be readily available to law enforcement as noted above. Thus, most communications will be accessible --

    - As data stored, often in plaintext, by communicating parties and available via court order;

    - Through stored decryption keys available via court order; or

    - Through other kinds of authorized surveillance.

4. Individual communications -- Similarly to business communications, the bulk of individual communications will be accessible to law enforcement through legal process in some manner. Fifth Amendment privileges for individuals may protect some of these communications.

The remaining problem for law enforcement can be narrowed to the real-time interception of communications without any notice to the party under surveillance. While this represents a problem for law enforcement, it is a narrow problem. There are currently only on the order of 1100 wiretaps conducted by law enforcement in the U.S. each year.[16]

The widespread use of compression algorithms, a vast array of text, audio, and video applications, and even 40-bit encryption have already made real-time electronic interception dramatically more difficult. The widespread use of strong encryption by our more sophisticated national enemies makes many of those interceptions impossible. The days of a vast positive signals intelligence operation are numbered, with or without U.S. export controls. We must find ways to help law enforcement and national security to adjust to this new world, without limiting effective privacy for individuals and businesses on the GII.

Moreover, the information economy presents new and powerful tools and opportunities for law enforcement. Online interaction leaves a detailed trail of electronic transactions, credit card purchases, online communications, and Web-based clickstream data presenting new traffic analysis opportunities. This information offers law enforcement unprecedented new tools to obtain evidence of criminal activity. The balance of power in an online world is tilting further towards law enforcement and away from individual liberty. Encryption may represent one of the rare opportunities to reclaim individual liberty in the face of the steady erosion of privacy and individual autonomy brought on by technology and the Information Age.

The federal government is granted the ability to monitor a specific telephone line. It has never been prospectively guaranteed the ability to intercept all communications of all individuals, and understand them. Wiretap targets have always been able to use other phones, or speak in unintelligible code. More importantly, the ability to hear a specific phone conversation is not nearly as invasive as the ability to intercept, without notice or consent, the full panoply of life online including health records, financial transactions, online entertainment, intimate letters and conversations. Law enforcement has been unable to justify this new, unwarranted expansion of surveillance capabilities sought through the control of encryption technologies.

Figure 1 -- Defining the Law Enforcement Problem: Access to Information Online

	Stored Data	Communications
Business Information	1. Available via court order just like unencrypted information. Keys for encrypted information are similarly available via court order.	3. Largely available: • As plaintext stored by communicating parties, available by court order. • Through decryption keys, available via court order. • Through other kinds of surveillance. Remaining problem in real-time interceptions without notice.
Individual Information	2. Available via court order in most cases, just as unencrypted information. In some situations, access to encryption keys may be protected by fifth Amendment privileges.	4. Largely available: • As plaintext stored by communicating parties, largely available by court order. • Through decryption keys, available via court order. • Through other kinds of surveillance. Remaining problem in real-time interceptions without notice.

VI. Conclusion

Current U.S. encryption policy fails to recognize the needs of users and the changes brought on by the Internet Age. The Internet is not like a phone system, so the extension of wiretapping authority to the Internet is inappropriate. The Internet is a global medium, so centralized control schemes like current U.S. encryption policy are likely to be ineffective. And the Internet makes U.S. Constitutional protections a local ordinance, so U.S. encryption policy should seek to guarantee the privacy and liberty of Americans in their communications outside of the United States.

In the current policy standoff between eroding law enforcement arguments and the emerging and acute privacy and security needs of the Information Age, Congressional

action is needed. Only Congress is in the position today to change U.S. encryption policy and get Americans the privacy and security tools they need. The private sector cannot do it. The Administration will not do it. The courts may do it, but not without a protracted struggle. Congress must act. CDT supports the legislative approaches embodied in S.1726, S.1587, and H.R. 3011. The Congress should act to immediately liberalize export controls and provide Americans on the Internet with the strong security and privacy they so badly need.

Footnotes

[1] Matt Blaze, et al., Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security: A Report by an ad hoc group of cryptographers and computer scientists, at 7 (1996) (hereinafter, "The Cryptographers' Report").

[2] John Perry Barlow is often attributed with the phrase, "In cyberspace, the First Amendment is a local ordinance."

[3] No. 96-1458 (E.D.Pa. 1996).

[4] See ALA v. Dept. of Justice, No. 96-1458 (E.D.Pa. 1996).

[5] National Research Council, Cryptography's Role in Securing the Information Society, at 8-6. (Hereinafter, "NRC Report".)

[6] NRC Report Summary at 12, 13.

[7] The Cryptographers' Report, at 5.

[8] NRC Report Summary at 1.

[9] Id. at 1

[10] Id. at 8

[11] "Had I but serv'd my God with half the zeal / I serv'd my king, he would not in mine age / Have left me naked to mine enemies." William Shakespeare, *Henry VIII*, act 3,

sc. 2.

[12] NRC Report at 8-7

[13] Cryptographer's Report at 5.

[14] Id. at 5. See also NRC Summary at 2.

[15] NRC Summary at 13.

[16] See NRC Report.