Testimony of JerryBerman

May 2, 1994
Speaker: Jerry Berman

Testimony

of

Jerry J. Berman, Executive Director
Electronic Frontier Foundation

before the

Committee on Science, Space and Technology

Subcommittee on Technology, Environment and
Aviation

U.S. House of Representatives

Hearing on

Communications and Computer Surveillance, Privacy
and Security

May 3, 1994

Mr. Chairman and Members of the Committee

I want to thank you for the opportunity to testify today on communications
and computer surveillance, privacy, and security policy. The Electronic Frontier Foundation (EFF) is a public interest membership organization dedicated to achieving the democratic potential of new communications and computer technology and works to protect civil liberties in new digital environments. EFF also coordinates the Digital Privacy and Security Working Group (DPSWG), a coalition of more than 50 computer, communications, and public interest organizations and associations working on communications privacy issues. The Working Group has strongly opposed the Administration's clipper chip and digital telephony proposals.

EFF is especially pleased that this subcommittee has taken an interest in these issues. It is our belief that Administration policy developed in this area threatens individual privacy rights, will thwart the development of the information infrastructure, and does not even meet the stated needs of law enforcement and national security agencies. A fresh and comprehensive look at these issues is needed.

I. Background on digital privacy and security policy

From the beginning of the 1992 Presidential campaign, President Clinton and Vice President Gore committed themselves to support the development of the National Information Infrastructure. They recognize that the "development of the NII can unleash an information revolution that will change forever the way people live, work, and interact with each other." They also know that the information infrastructure can only realize its potential if users feel confident about security measures available.

If allowed to reach its potential, this information infrastructure will carry vital personal information, such as health care records, private communications among friends and families, and personal financial transactions. The business community will transmit valuable information such as plans for new products, proprietary financial data, and other strategic communications. If communications in the new infrastructure are vulnerable, all of our lives and businesses would be subject to both damaging and costly invasion.

In launching its Information Infrastructure Task Force (IITF) the Clinton Administration recognized this when it declared that:

> The trustworthiness and security of communications channels and networks are essential to the success of the NII.... Electronic information systems can create new vulnerabilities. For example, electronic files can be broken into and copied from remote locations, and cellular phone conversations can be monitored easily. Yet these same systems, if properly designed, can offer greater security than less advanced communications channels. [_Agenda_for_Action_, 9]

Cryptography -- technology which allows encoding and decoding of messages -- is an absolutely essential part of the solution to information security and privacy needs in the Information Age. Without strong cryptography, no one will have the confidence to use networks to conduct business, to engage in commercial transactions electronically, or to transmit sensitive personal information. As the Administration foresees, we need

> network standards and transmission codes that facilitate interconnection and interoperation between networks, and ensure the privacy of persons and the security of information carried.... [_Agenda_for_Action_, 6]

While articulating these security and privacy needs, the Administration has also emphasized that the availability of strong encryption poses challenges to law enforcement and national security efforts. Though the vast majority of those who benefit from encryption will be law abiding citizens, some criminals will find ways to hide behind new technologies.

II. Current cryptography policy fails to meet the needs of the growing information infrastructure

As a solution to the conflict between the need for user privacy and the desire to ensure law enforcement access, the Administration has proposed that individuals and organizations who use encryption deposit a copy of their private key -- the means to decode any communications they send -- with the federal government.

In our view, this is not a balanced solution but one that undermines the need for security and privacy without resolving important law enforcement concerns. It is up to the Congress to send the Administration back to the drawing board.

A. Current Export Controls and New Clipper Proposal Stifle Innovation
---

Two factors are currently keeping strong encryption out of the reach of United States citizens and corporations. First, general uncertainty about what forms of cryptography will and will not be legal to produce in the future. Second, export controls make it economically impossible for US manufacturers that build products for the global marketplace to incorporate strong encryption for either the domestic or foreign markets. Despite this negative impact on the US market, export controls are decreasingly successful at limiting the foreign availability of strong encryption. A recent survey shows that of the more than 260 foreign encryption products now available globally, over 80 offer encryption which is stronger than what US companies are allowed to export. Export controls do constrain the US market, but the international market appears to be meeting its security needs without help from US industry. The introduction of Clipper fails to address the general uncertainty in the cryptography market. Announcement of a key escrow policy alone is not sufficient to get the stalled US cryptography market back on track.

B. The secrecy of the Clipper/Skipjack algorithm reduces public trust
---
and casts doubt on the voluntariness of the whole system

Many parties have already questioned the need for a secret algorithm, especially given the existence of robust, public-domain encryption techniques. The most common explanation given for use of a secret algorithm is the need to prevent users from bypassing the key escrow system proposed along with the Clipper Chip. Clipper has always been presented by the Administration as a voluntary option. But if the system is truly voluntary, why go to such lengths to ensure compliance with the escrow procedure?

C. Current plans for escrow system offer inadequate technical
---
security and insufficient legal protections for users

The implementation of a nationwide key escrow system is clearly a complex task. But preliminary plans available already indicate several areas of serious concern:

1. _No_legal_rights_for_escrow_users_: As currently written, the escrow procedures insulate the government escrow agents from any legal liability for unauthorized or negligent release of an individual's key. This is contrary to the very notion of an escrow system, which ordinarily would provide a legal remedy for the depositor whose deposit is released without authorization. If anything, escrow agents should be subject to strict liability for unauthorized disclosure of keys.

2. _No_stability_in_escrow_rules_: The Administration has

specifically declared that it will not seek to have the escrow procedures incorporated into legislation or official regulations. Without formalization of rules, users have no guaranty that subsequent administrations will follow the same rules or offer the users the same degree of protection. This will greatly reduce the trust in the system.

3. _Fixed_Key_: A cardinal rule of computer security is that encryption keys must be changed often. Since the Clipper keys are locked permanently into the chips, the keys can never be changed. This is a major technical weakness of the current proposal.

4. _Less_intrusive,_more_secure_escrow_alternatives_are_available_: The Clipper proposal represents only one of many possible kinds of key escrow systems. More security could be provided by having more than two escrow agents. And, in order to increase public trust, some or all of these agents could be non-governmental agencies, with the traditional fiduciary duties of an escrow agent.

D. Escrow Systems Threaten Fundamental Constitutional Values

The Administration, Congress, and the public ought to have the opportunity to consider the implications of limitations on cryptography from a constitutional perspective. A delicate balance between constitutional privacy rights and the needs of law enforcement has been crafted over the history of this country. We must act carefully as we face the constitutional challenges posed by new communication technologies.

Unraveling the current encryption policy tangle must begin with one threshold question: will there come a day when the federal government controls the domestic use of encryption through mandated key escrow schemes or outright prohibitions against the use of particular encryption technologies? Is Clipper the first step in this direction? A mandatory encryption regime raises profound constitutional questions.

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. So, 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, may well constitute a secret search, if the target is a virtual corporation or an individual whose "papers" are physically dispersed.

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, may a person's privacy be invaded by law enforcement without simultaneously informing that person.

Proposals to regulate the use of cryptography for the sake of law

enforcement efficiency should be viewed carefully in the centuries old tradition of privacy protection.

E. Voluntary escrow system will not meet law enforcement needs
---

Finally, despite all of the troubling aspects of the Clipper proposal, it is by no means clear that it will even solve the problems that law enforcement has identified. The major stated rationale for government intervention in the domestic encryption arena is to ensure that law enforcement has access to criminal communications, even if they are encrypted. Yet, a voluntary scheme seems inadequate to meet this goal. Criminals who seek to avoid interception and decryption of their communications would simply use another system, free from escrow

Copyright © 2013 by the Center for Democracy & Technology.
The content on this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Source URL: https://cdt.org/testimony/testimony-jerryberman