PREPARED STATEMENT OF JERRY BERMAN, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Security and Freedom Through Encryption (SAFE) Act
March 20, 1997 - House Judiciary Subcommittee on Courts and Intellectual Property

INTRODUCTION AND SUMMARY

The Center for Democracy and Technology (CDT) is pleased to have this opportunity once again to testify about encryption policy before the House Judiciary Committee. The Center wishes to make four basic points in its testimony:

U.S. encryption policy continues to deny computer users the essential technologies they need to prevent crime and protect themselves online. The Commerce Department regulations released since the last Judiciary Committee encryption hearing do very little to change the fundamental export control and key escrow-oriented policy that has limited the use of strong encryption to date.

Govemment-driven escrowed encryption is not a solution. Government-driven escrow systems are not trusted in the global marketplace, would impose significant new costs and risks on computer users, and would dramatically increase the surveillance capabilities of law enforcement at the expense of individual privacy and security.

Administration policy imposes tremendous costs with little benefit. U.S. policy will not stop criminals from using encryption to evade law enforcement surveillance. The Administration is imposing a costly new system on users with very limited clear benefits.

CDT supports the Security and Freedom through Encryption (SAFE) Act of 1997: The Administration has proven unwilling to change its basic approach to encryption policy. Congressional action is needed. The SAFE Act will liberalize export controls and help provide Americans with the strong security and privacy products they so badly need.

The Internet has vast potential to reinvigorate democracy, provide open access to information, and promote electronic commerce. The new interactive media can empower people to speak, be heard, participate in society, and share information. But the full promise of the Internet will not be met without a secure and trusted information infrastructure. Widespread use of encryption provides this needed security. CDT commends Representatives Robert Goodlatte, Zoe Lofgren, and the other co-sponsors of the SAFE Act for their continued commitment to this essential debate about the electronic privacy and security of Americans.

U.S. ENCRYPTION POLICY DENIES COMPUTER USERS ESSENTIAL CRIME-PREVENTING TECHNOLOGY

A. Encryption prevents crime and benefits law enforcement

The widespread use of encryption is of critical importance for public safety, national security, and law enforcement in the Information Age. As the FBI noted in its most recent Budget Request to Congress, ''the Cyberspace Achilles' heel is the NII [National Information Infrastructure].''(see footnote 2) The flow of sensitive information over the Internet leaves Americans increasingly vulnerable to the prying eyes of potential criminals, terrorists, or even foreign governments. Encryption addresses this problem by giving its users an easy and inexpensive means to protect sensitive information.

Encryption is particularly important because of the inherent difficulties of ensuring security in the new digital media. The open, decentralized architecture that is the Internet's greatest strength also makes it harder to secure. Internet communications often travel in the clear over many different computers in an unpredictable path, leaving them open for interception. An small message from Washington to Geneva might pass through New York one day or Nairobi the next—leaving it susceptible to interception in any country where lax privacy standards leave it unprotected. Encryption provides one of the only ways for computer users to guarantee that their sensitive data remains secure regardless of what network—or what country—it might pass through.

The need for encryption is becoming even more acute as sensitive information is increasingly finding its way into electronic form:

Individuals need encryption in order to trust the NII with private data such as home banking transactions, medical records, or personal communications.

Businesses need encryption to protect their own proprietary information as it flows across vulnerable global networks. As FBI Director Louis Freeh noted in Senate testimony last year, it is estimated that nearly $100 billion annually is lost to economic espionage—espionage that is increasingly taking the form of information theft through electronic means.

The country needs encryption to secure the vulnerable information infrastructure governing such sensitive applications as our utilities, financial markets, or air traffic control networks.

If broad participation in electronic commerce and the information society is to become a reality, the adoption of encryption in most phases of electronic existence will be required.(see footnote 3) Despite concerns about the use of encryption to evade law enforcement surveillance, the National Research Council found in its 1996 encryption study, ''On balance, the advantages of more widespread use of cryptography outweigh the disadvantages.''(see footnote 4)

B. Current U.S. policy prevents users from getting the encryption tools they need to protect security online

U.S. encryption policies continue to limit the availability of strong encryption products, both domestically and abroad. While the Administration has shifted jurisdiction of cryptographic exports to the Commerce Department, from the viewpoint of encryption users the policy remains essentially the same. Cold War-era export controls and unattractive key escrow proposals remain the centerpiece of Administration encryption policy. It is also notable that established Commerce Department rules for exemption to export control, such as the foreign availability of similar products, have been denied to encryption products.

As a whole, U.S. policy still exercises a coercive influence on the strength and availability of encryption. As a result of these policies, computer users have been unable to settle on an adequate encryption security standard.

Exportable 40-bit encryption is widely viewed as insecure; just last month a University of California graduate student 'broke' a forty-bit key using readily available campus resources within 3.5 hours.

Moderately stronger 56-bit encryption is only exportable, temporarily, for those willing to commit to development of escrow systems that have limited market demand. Moreover, even 56-bit systems are viewed as inadequate; a panel of expert cryptographers last year recommended that secure encryption systems use keys of 90-bits or more.(see footnote 5)

Stronger escrowed encryption systems are exportable, but there is limited market demand for escrow. Moreover, the escrow infrastructure needed to support these systems does not exist today and will take some time to develop.

Computer users remain at risk, awaiting the widespread deployment of encryption and facing increasing threats to their unprotected information.

GOVERNMENT-DRIVEN ESCROWED ENCRYPTION IS NOT A SOLUTION

The Administration has endorsed key escrow, ''key recovery,'' and other forms of escrowed encryption as its favored approach to encryption policy.(see footnote 6) While there is much debate about how much market interest there will eventually be for some form of escrowed encryption, the government continues to endorse key escrow that put the needs of law enforcement above the needs of computer users.

Escrowed encryption systems work in a variety of ways. Early forms relied on the storage of private keys by the government, or more recently by other trusted entities. Other systems—called ''key recovery'' by some—have escrow agents simply maintain the ability to recover the encryption keys for a particular encrypted communication session or stored file, requiring that such ''session keys'' be encrypted with the public key of the agent and included with the data. Still other systems rely on the splitting of keys between several agents, or on a combination of these techniques.

Key recovery systems share the essential elements of escrowed encryption: They provide a mechanism (external to the primary means of encryption and decryption) by which law enforcement or a third party can access the plain text of encrypted data.

There are serious differences between the types of escrow the market might demand and the government escrow requirements being imposed through U.S. regulations, including:

Government access without notice or consent—Law enforcement wants access to decrypted information without notice to, or consent of, the user.

Ubiquitous global adoption of escrowed encryption—Key escrow only meets law enforcement needs if it is widely used—both domestically and internationally—for the bulk of stored information and communications.

Access to communications as well as stored data—While there may be some market demand for access to stored data, there is virtually no market demand for recovery of communications.

High-speed, round-the-clock access—For example, the Commerce regulations require data recovery around the clock, within two hours of a request.

These requirements ultimately make government-driven escrowed encryption an unattractive and costly system for users.

A. Government-driven escrowed encryption is not a trusted global approach

The last several years have shown that escrowed encryption is not a trusted global approach to encryption. Since the introduction of the Clipper Chip in 1993, and continuing through the ''Clipper 2'' commercial key escrow and ''Clipper 3'' public key infrastructure proposals, computer users and the information industry have consistently rejected escrowed encryption.

Despite the Administration's best efforts, national governments have not globally endorsed key escrow solutions. In testimony before the Senate last summer, FBI Director Freeh argued that ''there is now an emerging opinion throughout the world that there is only one solution to this national and international public safety threat posed by conventional encryption—that is, key escrow encryption.'' In fact, there is evidence that no such opinion has emerged. The recently released OECD Cryptography Policy Guidelines specifically *do not* endorse key escrow; rather, they cautiously propose that ''national cryptography policies may allow lawful access to plaintext or cryptographic keys.'' (Emphasis added.) Without a significant consensus among national governments, there is no viable key escrow policy for law enforcement.

There is limited consumer demand for escrowed encryption. Major potential suppliers of encryption products have consistently maintained that the market does not want or trust the government's brand of escrowed encryption. Escrow providers have argued that encryption users will want escrow products to recover the keys to stored information in emergency situations—for example, the death of a key holder. While it is likely that there will be some demand for escrow for stored information, there is *virtually no consumer interest in escrow for encrypted communications.*(see footnote 7) Users will always have a plaintext copy of their communications; the only reason to escrow communications is to provide law enforcement or other third party access.

Escrowed encryption faces even greater burdens to acceptance internationally. Few international users can be expected to feel comfortable with key storage in the United States, which is required under U.S. export regulations until suitable multilateral agreements can be worked out. Since there are no Fourth Amendment protections outside of the U.S., escrowed encryption introduces new privacy concerns about what standards will govern access to encryption.

Finally, there are some application for which escrow will never be appropriate. For example, the AAAS has commented on the sensitive and increasingly important use of encryption by human rights advocates worldwide. ''if keys can be recovered by the U.S. government, why should human rights organizations whose entire function is defined by abusive governments trust that their information will remain secure?''(see footnote 8)

B. Escrowed encryption imposes substantial new costs and risks on computer users

Govemment-driven escrowed encryption will be expensive and less secure for users. Escrow will create new risks; for example, the large collections of key information stored by escrow agents will be an enticing new target for attack or espionage. Escrowed encryption will require a massive government infrastructure to approve products, monitor escrow agents, and provide law enforcement access. This high cost of maintaining a complex and highly secure escrow system will be shared by both users and the public, and will no doubt increase the cost of using encryption.

Escrowed encryption raises numerous unanswered privacy questions. What privacy standards will apply to the release of decryption keys among countries? Will the U.S. government honor requests from foreign governments for the keys of human rights workers or dissidents? How will the U.S. government guarantee the privacy of Americans communicating abroad with keys held in foreign countries? Without the answers to these questions, the Internet community will not and should not place its faith in an escrowed encryption infrastructure.

An escrow system of the sort contemplated by the Administration is orders of magnitude beyond the scale and scope of any similar secure system today. Far more information and experience is needed before the privacy and security of the information infrastructure is entrusted to an untested escrow infrastructure. As the NRC noted in its report, ''aggressive government promotion of escrowed encryption is not appropriate at this time.''

C. Guaranteed law enforcement access to all stored information and communications is a dramatic expansion of current surveillance capability

Congress and the courts have worked hard to strike a delicate balance between government surveillance and individual privacy. Key escrow would dramatically upset that balance. The federal government is currently granted the ability to monitor a specific telephone line. It has never been prospectively guaranteed the ability to access all stored information and intercept all communications—as escrowed encryption would.

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.

ADMINISTRATION POLICY IMPOSES TREMENDOUS COSTS WITH LITTLE BENEFIT

A. Current U.S. policy will not stop criminals from using encryption to evade law enforcement

Even if the marketplace were to adopt escrowed encryption as the Administration hopes, criminals will still be able to use strong encryption to evade law enforcement.

Strong, non-escrowed encryption is already available both inside and outside of the United States today. Foreign governments, terrorist, and criminals have access to these powerful tools and will be able to encrypt data despite continued export controls or escrowed encryption. Moreover, criminals within the United States will continue to have unfettered access to strong encryption under current regulations. Unless the Administration is planning to impose some form of domestic controls, criminals within the U.S. will always be able to use strong encryption.

Furthemmore, nothing in the Administration policies prevents users from ''superencrypting'' communications even within a key escrow framework. By encrypting information and then encrypting again using an escrow system, users will appear to have complied with escrow requirements while still storing data or communicating in a manner that cannot be intercepted, thwarting the entire law enforcement interest in imposing escrow.

B. The law enforcement problems with encryption are important but more limited than claimed

Law enforcement faces a real, but narrowly focused, problem with encryption. Congress should demand a full description of the law enforcement problems caused by encryption to date. Based on available information, however, it appears that the vast majority of encrypted information will be accessible to law enforcement by legal process. For example, businesses will still be required to produce the plaintext of encrypted business records under proper legal process. Stored information, corporate and business information, and even a great deal of electronic communication will most likely be largely available to law enforcement through legal process similar to that available today.

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.

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.

CONCLUSION

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 believes that immediate liberalization of export controls in the SAFE Act will help provide Americans on the Internet with the strong security and privacy they so badly need.

(Footnote 2 return)
Department of Justice, Federal Bureau of Investigation, FY 1998 Authorization and Budget Request to Congress, at A–72 (1997).

(Footnote 3 return)
The National Research Council's comprehensive 1996 report on cryptography includes a detailed examination of the rising importance of encryption. National Research Council, Cryptography's Role in Securing the Information Society (1996) (hereinafter, ''NRC Report'').

(Footnote 4 return)
NRC Report at 8–6.

(Footnote 5 return)
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).

(Footnote 6 return)
Many Interested parties have sought to draw sharp distinctions between Key recovery. and other forms of escrowed encryption. CDT believes that *key recovery is a form of escrowed encryption.*

(Footnote 7 return)

See, e.g., Microsoft Corporation, Comments on Bureau of Export Administration Interim Rule on Encryption Controls (Feb. 1997).

(Footnote 8 return)

American Association for the Advancement of Science, Comments on Bureau of Export Administration Interim Rule on Encryption Controls (Feb. 7, 1997).