PREPARED STATEMENT OF MARC ROTENBERG, DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

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

My name is Marc Rotenberg. I am director of the Electronic Privacy Information Center in Washington, DC. I recently served as the privacy expert for the Organization for Economic Cooperation and Development's panel on Cryptography Guidelines. I have also taught information privacy law at Georgetown University Law Center since 1991.

I am grateful for the opportunity to appear before the House Subcommittee today. I thank Representative Goodlatte and the other sponsors of the SAFE legislation for their willingness to tackle a complex but enormously important issue for users of the Internet both in the United States and around the world.

I. THE CHANGING ROLE OF CRYPTOGRAPHY

Across the Internet community, I believe that there is one message that users, experts, and associations wish to convey to this committee as it considers cryptography policy and that is that the current policy is in crisis and the time to for reform is now. Cryptographers from Whitfield Diffie to Bruce Schneier, Matt Blaze and Phil Zimmermann, associations such as the Internet Society and the Global Internet Liberty Campaign, and distinguished research groups such as the National Research Council have all said that the present attempt to control the development of cryptography by export control policy is mistaken and should end.

The reason is not hard to understand. The current system is a relic of a different era, a time when cryptography was controlled by the military and there was little practical commercial use and little public interest in the use of encryption. Our policies were developed in an era when encryption was largely the province of spies and soldiers. The policies of our government, which emphasized secrecy and control, were appropriate in their day. But the world has changed.

Today cryptography is used for everything from communication to commerce, from electronic publishing to new payment systems. It protects not only the confidentiality of communications, but also provides for authentication and verification. Encryption can even provide techniques for anonymous transactions that may one day promote commerce and protect privacy.

The electronic communications infrastructure is clearly no longer the exclusive domain of governments. Today's network carries not only diplomatic communique's and military plans as in an earlier day—it is the conduit for global electronic commerce, private correspondence and the most sensitive bits of personal information, including medical and financial records.

We also know that government attempts to force technological outcomes in this rapidly evolving area are invariably flawed. This is not surprising. When the government sacrifices the workings of the marketplace and consumer demand for its own best guess about what will work it gambles with our security. Even if we agreed with the Administration's goal, there is little reason to believe that the Administration's encryption strategy would succeed. Security technology is no longer the monopoly of the U.S. government—if, in fact, it ever was. The technological know-how is now global, and if the U.S. computer industry is not permitted to deliver these crucial products to the marketplace, other providers will quickly fill the void.

In such a world, the best policies are those that seek to adapt to changing circumstance. It would be foolhardy for our government not to anticipate that strong, unbreakable encryption will be widely available on the Internet. And it would be equally wrong to prevent American citizens and American businesses from making use of the best tools available to protect their sensitive information from potential criminal threats.

We are therefore in a period of transition when law must be updated to reflect new realities. Reforming the export control regime so that it reflects the need for good encryption in commercial products and to protect personal privacy is a sensible first step. Further delay is likely only to increase the risks to users and businesses.

II. THE PROBLEM WITH THE CURRENT POLICY

At the heart of our current debate over encryption policy is a simple question

whether it is wise to encourage the development of techniques to permit access by third parties to encrypted communications. The Administration thought this was a good idea when it initially recommended the Clipper scheme in 1993 and supported the proposal with a Presidential directive. Subsequently, the White House has conceded that Clipper was not a workable solution and dropped an elaborate experiment within the federal government after considerable cost to taxpayers.

Next came the key escrow proposal with the belief that third parties could take the place of the government and hold private keys. But concerns were raised about cost and implementation so a revised proposal called ''key recovery'' was recommended but that proposal also has problems. Now, the Administration is reluctant to say clearly whether it supports either key escrow or key recovery. It simply knows that it does not want good cryptography widely available.

The search for law enforcement's holy grail is an endless quest. New techniques to protect privacy on the Internet will in some circumstances make criminal investigations more difficult, just as the introduction of any new technology has posed challenges to law enforcement. But the benefits of the widespread adoption of encryption are significant and efforts to curtail development will impose great cost.

Much of the problem with the White House position is that it continues to place the interests of crime detection ahead of crime prevention and in this course has also sacrificed, privacy security, business development, and ultimately user confidence. As a result it has increasingly undermined the necessary trust that must be developed if the public is to make widespread use of these new system.

You cannot have ''escrow'' in Key Escrow where the keys will be disclosed without the knowledge of the user who deposited the keys.

You cannot have ''trust'' in Trusted Third Parties whose obligations to disclose your confidential information to the government may exceed their obligation to protect the privacy of your information.

You cannot have legitimate escrow ''Agents'' where the agent acts at the behest of the government and not the company in which the agent is employed.

Each one of these new proposals that seeks to hide the government's interest in monitoring private communication behind an ill-defined or ambiguous policy goal has only increased the level of public concern. And there is still more reason for concern. EPIC's Freedom of Information Act litigation produced FBI documents last year which show that key federal agencies concluded more than three years ago that the Clipper Chip key-escrow initiative will only succeed if alternative security techniques are outlawed and key-escrow is made mandatory.

The conclusions contained in the documents conflict with frequent Administration claims that use of Clipper technology will remain ''voluntary.'' Critics of the government's initiative, including EPIC, have long maintained that the Clipper key-escrow technique would only serve its stated purpose if made mandatory. According to the FBI documents, that view is shared by the Bureau, the National Security Agency (NSA) and the Department of Justice (DOJ).

In a briefing document titled ''Encryption: The Threat, Applications and Potential Solutions,'' and sent to the National Security Council in February 1993, the FBI, NSA and DOJ concluded that:

Technical solutions, such as they are, will only work if they are incorporated into all encryption products. To ensure that this occurs, legislation mandating the use of Government-approved encryption products or adherence to Government encryption criteria is required.

Likewise, an undated FBI report titled ''Impact of Emerging Telecommunications Technologies on Law Enforcement'' observes that ''[a]lthough the export of encryption products by the United States is controlled, domestic use is not regulated.'' The report concludes that ''a national policy embodied in legislation is needed.'' Such a policy, according to the FBI, must ensure ''real-time decryption by law enforcement'' and ''prohibit[] cryptography that cannot meet the Government standard.''

These documents demonstrate that the architects of the Administration's cryptography policy have always recognized that key-escrow must eventually be mandated. As privacy advocates and industry representatives have always said,

Clipper does little for law enforcement unless the alternatives are outlawed. But the impact of such a law would be sweeping as to be untenable. For this reason, we are particularly pleased with the provisions in SAFE that affirm the right to use and to sell any form of encryption.

There is no question that law enforcement has legitimate concerns. There will be lawful criminal investigations frustrated because some data was encrypted. But, as the distinguished National Research Council panel found, the widespread availability of strong encryption will also prevent crime.

The current policy of the Administration seeks by every conceivable means to establish a technique for government access private messages, whether stored in data files or sent in data transmission. Such a proposal is both unworkable and undesirable.

III. THE OECD

In the last few months you may have heard references to the positions of other government on cryptography. I cannot speak to the availability of encryption in other countries, but I can provide for the committee a first-hand account of how the OECD, the one international organization that has truly studied and wrestled with these issues, resolved the claims of government for lawful access.

During the past year I attended meetings of the OECD Expert Panel on Cryptography in Washington, in Paris, and in Canberra. I participated in the drafting and development of the Guidelines. I provided technical assistance to member governments that had questions regarding privacy matters and also helped make available many of the worlds leading experts in cryptography to the OECD for its deliberations.

Based on direct first-hand participation in the development of the OECD Guidelines as well as familiarity with the final document that will be presented to the Council of the OECD for adoption later this month, I can tell you that there is no consensus within the OECD to support the type of government access to private keys that the Administration is seeking.

In fact, the Administration delegate specifically asked the OECD member countries

whether they wished to endorse the key escrow concept. Only one country, a country that already has a legal regime requiring the creation of key escrow agents, supported the motion. Every other country that spoke made clear its objection to the endorsement of key escrow.

It is not simply that the OECD has rejected the key escrow proposal, the OECD went much further in the opposite direction and adopted one of the strongest statements in support of privacy that can be found anywhere in international law or policy. That principle says clearly:

The fundamental rights of individuals to privacy, including secrecy of communication and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.

The OECD recognized that some government ''may'' choose to promote lawful access to encrypted communications, indeed that is the policy that the Administration is currently pursuing, but beyond this acknowledgment there was little support for the key escrow effort.

I was particularly gratified that the OECD gave such a strong endorsement of privacy and chose not to endorse key escrow. I believe that promoting key escrow around the world may have a severe impact on the work of human rights organizations and threaten to shift a delicate balance between the rights of citizens and the authority of government in the wrong direction. Our own Department of State has reported each year on the growing use of electronic surveillance by governments against dissidents, journalists and human rights organizations. It is particularly important that democratic governments, and the United States in particular, send a clear message that the technologies of the emerging information infrastructure should not be designed to facilitate government surveillance of private communications.

IV. THE SAFE LEGISLATION

The SAFE legislation responds to the growing recognition that the current encryption policy is not workable and should be changed. For this reason, we believe it is an important step in a process that will eventually make available the strong

privacy tools and techniques necessary for the growth of commerce and the protection of freedom in the twenty-first century.

In particular, we support that the proposed sections 2802, 2803, 2803 to title 18 which would make clear that the freedom to use encryption, to sell encryption, and to avoid mandatory key escrow will be protected by the law of this country. Taken together, these three provisions establish the foundation of a new cryptography policy that could truly carry this country into the next century and provide the tools for privacy and security that are critical for users and businesses on the Internet.

The administration has said on numerous occasions, that there is no intent to regulate the domestic use of cryptography. If that is the case, then there can be no objection to enactment of these three critical provisions. Much of the current confusion that clouds US policy could be quickly resolved if the Administration would express its support for these changes.

At the same time, while we favor these three provision, we are very much concerned about section 2805 and ask the Subcommittee to carefully review this provision with the goal of narrowing it significantly or dropping it all together. Section 2805. which would make it a criminal act for ''Any person who willfully uses encryption in furtherance of the commission of a criminal offense,'' could have a series of unintended consequences that would easily undermine the other laudable provisions of the bill.

First, as I said during the hearings on the Computer Fraud and Abuse Act in 1989, I believe it is a mistake to create criminal penalties for the use of a particular technique or device. Such a provision tends to draw attention away from the underlying criminal act and casts a shadow over a technology that should rarely be feared. It may be the case that a ransom note from a typewriter poses a more difficult challenge for forensic investigators than a handwriting sample. But it would be a mistake to criminalize the use of a typewriter simply because it makes it more difficult to investigate crime in some circumstances.

Second, a provision which criminalizes the use of encryption, even in furtherance of a crime, would give prosecutors wide latitude to investigate activity where the only indicia of criminal conduct may be the mere presence of cryptography. In the digital

age we can no more view cryptography as the instrumentality of a crime, then we could the use of a pen or a paper clip in the current era.

Third, the provision could also operate as a substantial disincentive to the widespread adoption of strong cryptographic techniques. Recognizing as the National Research Council has, that the availability of strong encryption is one of the best ways to reduce the risk of crime and to promote public safety, the retention of this provision in the bill will send a mixed message to users and businesses that we want people to be free to use cryptography but we will be suspicious when it used.

If the concern is that cryptographic techniques may be used to obstruct access to evidence relevant to a criminal investigation, then the better approach may be to rely on other provisions in the criminal code, including sections relating to obstruction of justice, to address this problem.

Regarding Section 3, which would amend the Export Administration Act, we have doubts about the constitutionality of any form of export control on encryption. We have joined with Phil Karn in support of his litigation in the federal courts because we believe that the right to use cryptography is protected by the First Amendment. And, as you may be aware, Dr. Dan Bernstein has made substantial progress with a similar claim brought in federal court in California.

It is our belief that over time, as the courts will come to understand the public and commercial significance of cryptography and related techniques and that the President's authority to regulate this technology in the name of national security will become increasingly suspect.

Therefore, we are not prepared to concede that the Secretary of Commerce shall have ''exclusive authority to control the export of hardware, software, and technology for information security (including encryption)'' as the bill proposes. But we do believe that these changes will move encryption policy in the right direction by ensuring that strong cryptography will be more widely available.

In summary, we support the legislation and applaud the sponsors and the committee for your work on this matter, but we urge you to look carefully at the proposed section 2805 and see whether there may be a more limited way to address this problem.