PREPARED STATEMENT OF ROBERTA KATZ, SENIOR VICE PRESIDENT, GENERAL COUNSEL, AND SECRETARY, NETSCAPE COMMUNICATIONS CORP., ON BEHALF OF INFORMATION TECHNOLOGY ASSOCIATION AND SOFTWARE PUBLISHERS ASSOCIATION

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

I. INTRODUCTION

My name is Roberta Katz. I am the Senior Vice President, General Counsel and Secretary of Netscape Communications Corporation. I am pleased to state for the record that I am also here as a witness on behalf of the Information Technology Association (ITAA), an international organization of several thousand information technology product and service providers, and on behalf of the Software Publishers Association (SPA), an international organization dedicated to the protection of intellectual property and the interests of software publishers small and large.

It is an honor and a privilege to testify before the Committee today. I submit to you that while it may not seem like it at first glance, the subject of information security is one of the most important issues facing our society and, therefore, the Congress.

I believe we are at a critical juncture with regard to the Administration's policies on the subject of information security. In a narrow sense the issue is about the export of encryption technology by U.S. firms, but the ramifications of these policies are much broader, so I commend you for having this important hearing early in the 105th Congress. I believe it is time that we move the debate on this subject. We want to address in a positive way the degree to which the marketplace has responded as the Administration would have hoped, and the hope that market driven changes in the infrastructure have the concomitant benefit of addressing law enforcement and national security concerns.

If the government truly intends to micromanage a key escrow or key recovery infrastructure, its policies will be doomed to failure. Indeed, the government has accomplished all that it can realistically accomplish through the use of existing export

controls, as it has pushed U.S. industry into building key-recovery programs to create and meet market demand. But there are limits to what the government can accomplish in the marketplace. We have stated consistently that there would be demonstrable demand for voluntary deployment of key recovery products for commercial use. The debate of the last year has undoubtedly accelerated this demand. At the same time there is clearly a significant demand for non-recovery products. Try as it might, the government simply doesn't have the ability to eliminate demand for non-key-recovery products.

The Administration has, through its actions, guaranteed that people who want key recovery products can choose from many capable suppliers. Without broad agreement enforceable through a multilateral organization, a world-wide government approved key recovery system will not come to fruition. Let me say again: More cannot be accomplished through the existing scheme of export controls. The Administration should take credit where credit is due, and let the marketplace develop the solutions going forward.

We will never have a perfect world. A perfect world certainly does not exist with respect to wiretap ability in telephony markets; there will surely not be a perfect solution with respect to data. It is now time to clearly recognize that and to move on. With an ear to the marketplace and our willingness to share technical information about our products with appropriate government agencies, we can and will develop solutions that are both successful in the world marketplace and provide aid to law enforcement authorities. We must change the policy of this country so that companies like mine can get on with the business of selling our products around the world and we need legislation to accomplish this. We support H.R. 695 wholeheartedly. It will bring overdue relief and allow U.S. industry to compete openly and fairly with other international developers and providers of encryption hardware and software products and services.

II. WHY THE ADMINISTRATION'S POLICIES AND REGULATIONS DO NOT WORK

A. The Administration's Current Policy: Grudging Acceptance of Yesterday's Technology While the Rest of the World Moves Ahead

The Administration's regulations try to force computer code to include some form of key recovery by restricting sale of strong encryption outside of the U.S. and Canada. Other witnesses will stress that companies have filed applications under the new regulations, and suggest this validates the new regulatory approach. It is true

that some see new market opportunities, and other companies must respond to competitive pressures. Some companies will attempt to satisfy the new regulatory regime while seeking broader changes in the law. The primary reason the regulations will not work is this: while U.S. companies attempt to comply with regulations, companies such as Stronghold in the U.K., Brokat in Germany, Siemens Nixdorf in Germany and NTT in Japan are providing strong, sophisticated encryption throughout the world in a manner unimpeded by government regulation.

The current US policy on encryption exports provides companies with a 2-year interim period during which companies can export products including 56-bit DES (without key recovery) provided the following is met:

The company supplies the government (Bureau of Export Administration, Commerce Department) with a business plan outlining a 2-year plan for implementing a key recovery mechanism within the product(s) in question;

The 2-year plan should outline the proposed technical solution for key recovery, some schedules and milestones for delivering key recovery enabled products; and

Provide the government with a 6-month progress report.

The policy does not necessarily require a company to implement any specific key recovery method, rather the companies are asked to provide the plan that would work for their products and market. The policy also suggests that after key recovery has been implemented and approved by the various government agencies, the products can be exported with basically unlimited key length, provided the encryption algorithms are known. Hackers and computing power make a 56 bit solution totally vulnerable today. Cryptographers have reported as recently as last year that the minimum necessary key bit length is at least 90. Customers demand to have at least the same level of strength as U.S. customers. For communicated data that is 128 bit SSL. With non-U.S. developers such as Stronghold and Siemens Nixdorf producing and selling 128 bit SSL the benchmark is 128. There is no telling what the benchmark may be in just two years.

There is an inverse relationship between the degree of government control of information security features and the value of those features. Foreign customers and governments grow suspicious of products that fit too neatly into a U.S. government standard. They fear that it has some sort of back door for governments to creep in through or that the U.S. policy favors U.S. firms that have gone along with the policy through and through and will block out non-U.S. firms in some way. Whether or not

such suspicions are substantial or permanent they are interfering with the development of the marketplace and they taint the image of U.S. firms trying to do business overseas.

B. Regulatory Processes and Timetables Stifle Businesses Who Must Operate on ''Internet Time''

To date the U.S. industry has had to suffer from uncertainty—the Administration has changed its policies four times in as many years—and from costly and risky regulatory burdens. Small U.S. firms cannot afford the licensing process and it is inefficient for any firm to have to file and argue for a license for each non-U.S. customer. This is especially true for start-up companies like mine in relatively new industries which operate at a fast pace called ''Internet time.'' Now we have yet another regulatory experiment aimed at ''skewing the marketplace.''

The regulations require industry to participate in a two year interim process. In two years time, four to five product cycles will have come and gone. We will be on version eight or nine of our software by the end of this experiment in industrial policy making. It is our view that government regulations are retarding the deployment of market-driven solutions and technologies which might actually do more to the achieve the goals of the Administration than the regulations themselves.

The experimental and evolving nature of U.S. regulations undermine their effectiveness and hamper U.S. businesses. Mr. Reinsch told industry representatives last year at a meeting in Silicon Valley that if they don't work, the Administration would have to try something else. Also, once a license to export is obtained under the current regulations, there is nothing to prevent the license from being taken away for no clear reason, as the regulations and their process are not reviewable in Federal Court or under the Administrative Procedures Act. For this reason alone, Pro-CODE is critical. Netscape cannot afford to invest in a technology that is one day exportable and then another not. When our customers make the commitment to become a Netscape customer, they want to know that we will be there year in and year out to support the products we sell them, no matter what part of the world they are doing business in.

C. Current Polices Fail Cost-Benefit Analysis.

The cost of doing business under the U.S. policy and regulations is not defensible, and greatly outweighs the benefits of the regulations. We believe the benefits of the regulations have largely been maximized to date—that is, that the market for key

recovery products has been accelerated. The costs to develop and operate an infrastructure are truly not known because, to our knowledge, nothing of this dimension has been attempted. But it is clear that those costs would be astronomical. Many of the products and services necessary to support a global public key recovery infrastructure simply do not yet exist or are only in their early stages of development.

D. Standards and U.S. Law Enforcement Interests

The Administration can incorrectly take credit for making encryption an important issue. By forcing industry to lose market leadership and sales over the past three years, industry has had to make a complex topic very plain, simple and immediate. Without the deployment of strong and sophisticated information security, both law enforcement and industry suffer. Neither wins. If there is no sophisticated encryption, data may be in the clear but it can be authenticated to and inadvertently shared with an unintended user. Without strong, interoperable encryption available world-wide, companies and individuals are unable to protect their intellectual property or private communications in the global information society.

Currently available key recovery products meet customers need for e-mail and stored data comprise an part of an infrastructure which is fortuitously consistent with the need for lawful access when appropriate procedures are followed. These features allow an employer to have access to encrypted data immediately if, for example, an employee dies, defects to a different firm, steals proprietary information, or vanishes. These functions can be achieved without mandating that keys to unlock the information be escrowed to a particular kind of third party, in a specific country, using a specific algorithm, or using government prescribed key recovery features.

Secure Sockets Layer (''SSL'') is the Internet industry standard for securing communications. The SSL protocol provides data recovery capabilities that law enforcement can utilize to get access to encrypted data through the server. The use of strong cryptography, in fact, provides strong authentication for users which, in turn, actually increases the possibility for law enforcement to obtain data pursuant to lawful procedures and to match this data to the proper person.

If the session is unencrypted, the parties can not be authoritatively identified. In telephony, wiretapping data in original form naturally contains individual identification information (e.g., the sound of a person's voice can be matched), but

trying to wiretap an SSL session is not at all the same. The ability to intercept the data midstream and decrypt it in real time would not necessarily allow the data to be linked to a particular person. Even if a wiretap could be made on a telephone line that was being used to dial out to the Internet via a modem, it is not clear that a useful law enforcement objective would be achieved. If this wiretap were able to collect the keystrokes in the clear or decrypt them, and if such keystrokes indicated that the communicant were typing in a URL to a secure server in the Cayman Islands such as ''www.cashlaundry.com,'' one cannot prove from the wiretap who committed those keystrokes to the keyboard. A communicant could be mobile, use wireless technology, or route their connections through a proxy, or spoof an Internet protocol (IP) address (i.e., domain name) in order to avoid detection. Attaching identity to the client end of communications on the Internet is extremely difficult. We submit that SSL does not on balance undermine law enforcement. Rather, a security feature like SSL allows the communicants to be authenticated to the session, and the session authenticated to a particular server, which is of considerable value to law enforcement. It is one of the reasons we believe that deployment of a secure and sophisticated infrastructure will come to be viewed as a deterrent to technology-savvy criminals.

Key recoverability is an added value feature for email and certain stored data systems. In contrast, there is no user demand for this feature in the context of transmission of point to point communications. We believe that a system that attempts to escrow SSL communication session keys cannot work even if it were somehow brought into existence. Billions of session keys are being created and discarded every day, and it is inconceivable that a system could be designed which would allow useful interception of information in transit. Additionally, such a system would involve far too many additional communications, too many added key exchanges, and too many new points of attack for hackers to be useful, practical or secure.

The Internet only exists because of open, non-proprietary, non-secret, interoperable standards. Current U.S. policies make it increasingly likely that foreign manufacturers will set standards inconsistent with these objectives. Foreign manufacturers of strong encryption software such as Stronghold and Siemens market themselves by stressing the opportunities presented to them by U.S. policies which hurt us: They state that their products are available world-wide with a full 128

bit SSL function and distinguish themselves from U.S. companies like Netscape and Microsoft that are limited by the U.S. government to trivially-cracked 40 bits.

For the time being, Stronghold and other non-U.S. developers build on open standards like SSL, but there is no guarantee open standards will prevail or survive. The requirement for U.S. firms to participate in shaping the implementation of open standards as well as the standards for other components of the architecture of information security such as certificates and certificate authorities is critical. If implementation of standards is driven by non-U.S. product, there is not certainty that those developers will have any sympathy for law enforcement concerns or consumer protection, especially the concerns of U.S. law enforcement authorities.

Open, interoperable, global technical standards are the best way to provide a robust and sophisticated infrastructure that can address and balance the needs of the market with public safety. At present, U.S. policy and regulations prohibit Netscape engineers from talking to Siemens Nixdorf engineers about how to make sure each firm's implementation of SSL and SMIME interoperate with respect to how the data can be recovered and the user can be authenticated in an Intranet environment. The only way such technical discussions can occur is if Netscape files for a license and waits for approval—a bureaucratic process that is costly, uncertain and possibly undermines the business relationship. The non-U.S. firm is handicapped by the uncertainty, delay and restrictions inherent in the U.S. regulatory bottleneck. Our foreign customers are law abiding citizens living in countries whose national security and law enforcement communities cooperate with their U.S. counterparts. Although we are trying to help them establish systems that can provide this critical balance, government licensing procedures hinder our ability to provide this balance.

E. Unilateral Destabilization

Foreign governments have expressed the view that the U.S. policy represents a ''unilateral destabilization of a traditionally multilateral, cooperative process.'' The lobbying efforts of Ambassador Aaron and his predecessors are of particular concern to us. Ambassador Aaron has been given the job of convincing sometimes reluctant foreign governments to adopt the U.S. key recovery plan. Simultaneously, the Administration has disseminated the view on Capitol Hill and elsewhere that the rest of the world has adopted or is moving towards adoption of the U.S. plan. The lobbying strategy of the Administration has even included telling members of Congress that foreign governments are rapidly adopting their own domestic and

import restrictions. This process is not only skewed, but some of this information being disseminated is just not true.

We are trying to compete in a global marketplace. Not only won't our government help us sell our products to foreign customers, as we suggest would be more appropriate behavior, they keep us in the dark about just exactly what they are doing in their world-wide campaign. The much discussed National Research Council report, released in 1996, concluded that there was no reason to work through these policies in the darkness of government secrecy. The use of U.S. tax dollars to secretly undermine the interests of U.S. industry is confusing and frustrating to us. We appreciate the fact that Ambassador Aaron has come to our company to share information, and believe he plays a valuable role in educating industry about law enforcement rules and procedures in non-U.S. jurisdictions.

III. CURRENT RESTRICTIONS DO NOT ACHIEVE STATED OBJECTIVES

Netscape or Wal-Mart or Sears can sell any product to anybody in the world unless there is a compelling policy reason to limit that sale, and if the practical means used to enforce that policy are effective. In this case, the goal of any restrictions would be to keep something out of the hands of criminals or terrorists. We support the goal, but we can't conceive of any reason why the government still believes that the U.S. export controls prevent these benign products from coming into possession of bad people. Imagine that you are part of a criminal enterprise and that you wanted to be able to communicate securely so that the law enforcement agencies couldn't listen in. First, you might take a walk in the park and simply have a conversation. That would be hard for the government to listen in on. But if you wanted to communicate over a data network, you might obtain some product with information security features. You could walk into a store in America and buy anything you want, or you could simply download it off the Internet. If the government imposed a mandatory key recovery program supported by all governments in the world, which is unlikely, a criminal or terrorist would simply re-encrypt his communications. So the result of a key recovery system, would not be that U.S. authorities can listen in on terrorist or criminal communications. It will mean that the communicants will take other steps to avoid detection. There is a tempting story that strict export controls will allow meaningful, real time interception of communications and that all bad actions will be thwarted—but unfortunately, that story doesn't withstand scrutiny.

Computer fraud and computer-related crime rank high among law enforcement

concerns. In this context, the government surely agrees that information security features are not a problem; they are the solution to a problem. The FBI has testified about the threat of economic espionage, and expressed concern that, in the post-Cold War era, foreign governments have increasingly shifted much of their intelligence focus to the business sector. Hostile intelligence efforts to pry secrets from corporate America presents a clear threat to our economic and national security. The key escrow and key recovery solutions advanced by the Administration would increase the likelihood that foreign governments and their agents would have access to the intellectual property and trade secrets of U.S. companies.

We do not want to be alarmists, but it is worth repeating that government computer systems, including those at the Pentagon, have been repeatedly penetrated. Our power grid, gas and oil pipelines, stock exchanges and related intellectual property are among potential civilian targets. It is no secret that the supposedly confidential medical records of our citizens are often maintained on insecure and vulnerable networks. Information security embedded into the infrastructure is the solution to these problems.

I believe the Administration has conceded that all but the dumbest criminals and terrorists will be able to take steps to avoid detection, even under a key recovery scheme. But the Administrations has maintained that the real purpose of a key escrow or key recovery system is to obtain communications between terrorists and criminals and legitimate institutions such as banks. The suggestion is that without a government mandated key recovery system, a criminal could conduct a transaction with a financial institution or commercial enterprise and could somehow encrypt the communication to avoid detection by law enforcement. That rationale for export controls simply does not withstand scrutiny.

First, export controls and communications between criminals and financial institutions are simply different subjects. Second, Banks and other users of communications technologies must adopt systems which allow for data recovery. If they want to stay in business very long, they won't give the keys to government agents in advance, but instead they will adopt their own procedures that provide for lawful access. Criminals can't hide the fact that transactions have taken place with legitimate institutions simply by using encryption software. Legitimate institutions maintain records that are susceptible to lawful surveillance, and such institutions obviously maintain decryption keys. Law enforcement authorities do not need key

recovery schemes to determine that a communication with a financial institution has occurred, the location and identity of the communicant (assuming a secure environment) and the nature of the communications. If this ''catch the criminal when he goes to the bank'' is really the underlying rationale for the export controls, the restrictions should be lifted immediately.

Netscape is an American company and we're proud to say we are the fastest growing software company in history. We regularly communicate with top officials at the NSA, the FBI and other government agencies about our products. We are willing to share certain information with the government (and other governments, when we can get an export license from our own government) so they can do their jobs and better understand the latest technology. We do not want to hide anything, except that we must be cautious about disclosing proprietary information that would find its way into the hands of our competitors.

V. CONCLUSION

The new policy of the Administration has been in place for nearly three months and it is clear, from the comments filed on the Commerce Department regulations to the White House's ''Framework for Global Electronic Commerce'' section on security, that the Administration's policy is widely unpopular. When Ira Magaziner, Senior Policy Advisor to the President, spoke last week in San Francisco at a conference called ''Computers, Freedom and Privacy,'' he acknowledged that the security section, a direct reflection of the Administration's policy and regulations of encryption, was not supported by 90 to 95% of the comments received. Last year Administration officials often used the Organization for Economic Cooperation and Development (OECD) and its work on cryptography guidelines to somehow support the notion that there was international consensus for the U.S. government position on key escrow and recovery. In fact, at the last substantive meeting on the guidelines in December in Paris, the U.S. delegation's proposals to include an explicit reference to key recovery in the guidelines was rejected.

Senior Netscape executives and employees have met and continue to meet with the President and other senior officials of the Administration. We acknowledge they do not see it our way yet, but we are convinced the shortcomings of their current plan will become apparent. And then what? Will it lead to yet another series of experimental regulations? We suggest the regulatory futility must stop. The Administration has accomplished all that it is going to with the existing export

control regime. They will not succeed if they proceed with the implicit goal of mandating that every customer in the world use U.S. key recovery products or if, as has been suggested, they pursue domestic controls on information security products.

Netscape strongly supports H.R. 695 and we look forward to its swift enactment this year, which will preserve our strategic interests in leading the development of the information age.

CURBS ON ENCRYPTION CRACKED

U.S. restrictions over the export of 128-bit key encryption technology remain a source of frustration for European and other organizations which need the highest security for their Internet and intranet applications.

Now Siemens Nixdorf Informationssysteme, part of the German Siemens group, has developed a new product called TrustedWeb, which incorporates a 128-bit public key/private key developed by Dublin-based Systems Engineering—a joint venture between SNI and its parent.

''TrustedWeb is an independent European product and hence is not subject to the export restriction imposed by the U.S. government in relation to encryption software,'' says Siemens Nixdorf.

The software, which comprises three components, is expected to be used with conventional firewall software both to protect corporate intranets against unauthorized external access, and to prevent internal access to confidential Web pages or application data.

Siemens Nixdorf Ireland will market the software worldwide over the Web.

TrustedWeb:http://www.TrustedWeb.com