**PREPARED STATEMENT OF JONATHAN SEYBOLD, CHAIRMAN, EXECUTIVE COMMITTEE, AND DIRECTOR, PRETTY GOOD PRIVACY, INC.**

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

Mr. Chairman and Members of the Committee, I appreciate the opportunity to testify on Mr. Goodlatte's bill, the Security and Freedom through Encryption Act of 1997. I would also like to take this opportunity to thank Mr. Goodlatte for his leadership on the issue of liberalizing controls on the export of encryption technology. PGP strongly supports legislation, such as the SAFE Act, that protects the sale and use of encryption technology domestically and liberalizes controls on the export of strong encryption.

ABOUT PRETTY GOOD PRIVACY

I am Chairman of the Executive Committee and a co-founder of Pretty Good Privacy, Incorporated. PGP provides corporate and individual consumers with a broad array of privacy and security solutions that prevent the risk of unauthorized access to digital privacy.

Pretty Good Privacy was co-founded by myself, Dan Lynch (Chairman of CyberCash), and Philip Zimmermann, the creator of PGP, our flagship product. PGP—which we now call PGPmail—is a public key encryption software package for the protection of electronic mail.

PGP's products address three interrelated aspects of privacy. The first aspect is *encryption,* which prevents unauthorized individuals or organizations from reading intercepted files. Encryption basically scrambles a message, allowing only the intended recipient to unscramble the message with the use of a key.

The second aspect of privacy is *authentication,* which ensures that a message received originated from the correct source, and has not been altered in transition. Our products let senders include a unique digital signature with a transmission, proving that they originated the message, and that it has not been altered.

The third aspect of privacy is *anonymity,* which limits the extent to which an individual or corporation's identity can be tracked electronically over the Internet. This allows a company or individual to explore the Internet freely, without fear that

they are sending out valuable information about themselves in the process.

Almost half of the U.S. Fortune 100 companies, and over 2 million individuals worldwide, use Pretty Good Privacy to guarantee the confidentiality and authenticity of their communications and transactions.

CURRENT ENCRYPTION POLICY

Last December, the Clinton Administration made an attempt to liberalize export controls on encryption technology and address law enforcement concerns by publishing new regulations covering the export of encryption. Under these new laws, companies may receive permission to export strong encryption only if government access to the keys is facilitated through a government-approved escrow arrangement.

We strongly oppose this government-mandated solution, for three primary reasons: 1). It threatens the competitiveness of U.S. corporations such as PGP that are the world leaders in encryption technology. 2). It ignores the serious security concerns of consumers of encryption products. 3). It compromises the privacy rights of individuals worldwide, thus prohibiting the spread of democracy.

Representative Goodlatte's (R–VA) Security and Freedom through Encryption Act of 1997, which I will talk about in more detail momentarily, makes great strides toward correcting the inadequacies of the Administration's policy.

*1. The Administration's Policy Threatens the Competitiveness of U.S. Corporations*

The Administration's key recovery mandate wrongly assumes that the market will accept a governmental, non-market driven approach to encryption. Based on our customers' response, we do not believe that a significant market exists for encryption designed to facilitate government access to keys. Companies from other countries, including Japan and South Africa, are developing and exporting strong encryption without government-mandated escrow requirements. It is far too late to control the development overseas of this technology. That horse is already out of the team. If the Administration's policy is maintained, consumers worldwide will choose to purchase foreign encryption technology, because it will be strong, readily available, and market driven. But most importantly, they will buy foreign encryption technology because buying U.S. encryption will be like *buying a safe to which another person has the key or combination.*

The Clinton Administration argues that it can allay these competitiveness concerns by leveling the playing field, ie., convincing our allies not to export their strong

encryption technology without an escrow system. If past is prologue, such efforts will be fruitless. In the past, the U.S. government has been unsuccessful in its efforts to convince even some of our closest allies, such as Germany, France and Japan, to control the export of high technology. In the days of CoCom (the Coordinating Committee for Multilateral Export Controls), U.S. controls on technology exports were almost always more restrictive than those of other nations. This led to the loss of key sales to foreign competitors in technologies such as supercomputers and telecommunications equipment, where U.S. industry was technologically dominant but hindered by outdated export controls.

Maintenance of the Administration's key recovery mandate will cripple U.S. leadership in the worldwide market for encryption technology.

The Administration's policy negatively affects not only the international competitiveness of U.S. encryption technology companies, but also puts U.S. companies at a competitive disadvantage in their own market. Creating and deploying two encryption standards—one for the domestic market and one for the international market—is expensive and burdensome for encryption technology suppliers, putting them at a disadvantage vis-a-vis their international competitors. In addition, maintaining two standards is burdensome for corporate users of encryption technology who must communicate both domestically and internationally.

*2. The Administration's Policy Ignores the Security Concerns of Users of Encryption Technology*

The theft, misappropriation and wrongful receipt of intellectual property and technology, particularly by foreign governments and their agents, directly threatens the development and making of the products that flow from that information.... For an individual, a stolen plan, process or valuable idea may mean the loss of their livelihood; for a corporation, it could mean lost contracts, smaller market share, increased expenses and even bankruptcy; and, for our Nation, a weakened economic capability, a diminished political stature, and loss of our technological superiority. Most estimates place the losses to businesses from theft and misappropriation of proprietary information at billions of dollars a year.

Within this evolving global environment in which information is created and shared instantaneously over national and global information highways—an environment in which technology is critical to all types of industry—both the opportunities and motives for engaging in economic espionage are increasing.—*FBI Director, Louis*

*Freeh, Testimony before the Senate, Select Committee on Intelligence, February 28, 1996.*

As these quotes from FBI Director Louis Freeh explain, it is increasingly difficult to protect privacy and confidentiality in the information age, and increasingly important to do so. The cost of corporate and individual exposure is mounting daily. The U.S. Department of Justice estimates that annual losses related to computer security breaches in the U.S. could be as high as $7 billion. As the electronic transactions and communications increase, so will the losses, unless companies and individuals are given the tools to protect themselves from security breaches. *Law enforcement officials are trying to combat these nefarious practices, but they are like doctors who try to treat the symptoms of disease, rather than giving the population a readily available vaccine.* The Administration policy withholds the vaccine—encryption technology—that companies and individuals need to protect their confidential information, from espionage, hackers, and criminals.

The Administration proposal does this by prohibiting the export and overseas use of U.S. encryption technology—even between U.S. companies and their wholly owned foreign subsidiaries—without a special license, which is virtually impossible to get for strong encryption products. Companies and individuals should have the right to protect their private and confidential transactions regardless of whether the transactions are conducted domestically or across international borders.

*3. The Administration's Policy Compromises Important Privacy Rights of Individuals, and Inhibits the Spread of Democracy*

Cryptography is the cornerstone of the protection of individual privacy in the Information Age. As face-to-face conversations are replaced by teleconferencing, paper mail is replaced by electronic mail, and cash transactions are being replaced by electronic commerce—it becomes increasingly easy for others to eavesdrop on our private communications. This has phenomenal implications for individual rights, particularly as they relate to potentially repressive governments, whose ability to monitor and collect information on citizens has grown exponentially in the Information Age.

The Justice Department argues that its ability to investigate and prosecute criminal activity is strengthened by export controls on encryption. *It could also be argued that law enforcement's ability to investigate and prosecute criminal activity would be strengthened by the repeal of nearly every one of the first ten amendments to the*

*Constitution.* Of course, no one advocates that approach. Our forefathers understood that Democracy requires a balance in favor of individual rights, and they designed the U.S. Constitution and the Bill of Rights to protect that balance.

Individual rights should not be enjoyed only by Americans, however. As the leaders and promoters of Democracy worldwide, *it is our responsibility not only to protect the rights of American individuals to privacy, but also to foster the protection of those rights for citizens of the rest of the world.* Phil Zimmermann, the creator of PGP, regularly receives e-mail messages from individuals and organizations which use PGPmail overseas. It is used by witnesses to report human rights abuses in repressive countries. It is used by Amnesty International. In October 1993, when the Russian government was shelling the Parliament building, Phil received a message from a man in Latvia who said:

*Phil, I wish you to know: let it never be, but if dictatorship takes over Russia your PGP is widespread from Baltic to Far East now and will help democratic people if necessary. Thanks.*

Pretty Good Privacy and other U.S. corporations have the technology to export the individual right to private communications, thus contributing to the global spread of Democracy. It is essential that we be allowed to do so.

*The Security and Freedom through Encryption Act of 1997*

To correct these flaws in the current policy, we support H.R. 695, the SAFE Act. The SAFE Act significantly liberalizes export controls on encryption technology, addressing many of our competitiveness concerns. The SAFE Act also prohibits mandatory key escrow and codifies the right of U.S. citizens to use encryption, addressing important security and privacy concerns.

The SAFE Act contains one section in particular that PGP finds very disturbing. We are concerned that Section 2805 stigmatizes the use of encryption. The section provides additional penalties for ''any person who willfully uses encryption in the furtherance of the commission of a criminal offense ...''

PGP would like the language modified to clarify that encryption is not a crime in and of itself, that a person must be *convicted* of a crime before additional penalties can be imposed for the use of encryption, and that a person must be willfully using encryption with the intent of hiding evidence of a crime before the additional

penalties would apply.

We are happy to work with the subcommittee staff, and with Mr. Goodlatte's office, on the specific language.

There are three other issues that we would like addressed in the SAFE Act:

1. Some of the terminology is confusing, and should be changed for simplicity's sake. For example, the use of the terms ''generally available'' is different in the legislation than it is understood under Export Administration Regulations. We would prefer that the SAFE Act use the EAR term ''mass market'' software.
2. ''De minimis'' exceptions should be reinstated for both hardware and software. The Administration's Executive Order states that foreign origin products that contain even a ''de minimis'' amount of U.S.-origin content are subject to export controls.
3. The foreign availability provisions that apply to hardware in the bill should also apply to software.

Again, we look forward to working with the staff to address these issues, and to move this legislation toward passage. Thank you again for the opportunity to testify, and I am pleased to answer any questions.