

**PREPARED STATEMENT OF THOMAS R. MOREHOUSE, PRESIDENT
AND CEO, SOURCEFILE**

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, thank you for this opportunity to share my views on commerce in encryption products. I am honored to appear before you today. As the National Research Council's 1996 study on Cryptography's Role in Securing the Information Society says, we have a policy crisis, not a technology crisis—the technology is here. Thus this hearing is both timely and extremely important.

My company, SourceFile, through its SourceKey division, is the only company authorized by the United States government to provide key recovery services for export-approved products containing strong encryption. Companies look to SourceFile as a trusted third party to protect their copyrights, trade secrets and other intellectual property. Through our source code escrow services, Fortune 1000 companies rely on us to protect their investment in mission-critical computer software. Thus, we have a keen interest in public policy that protects private intellectual property. As American citizens, we are also concerned about safeguarding our privacy, protecting our national security and preventing crime.

The debate over encryption export policy involves parties with three distinct interests: civil libertarians and free speech advocates, business and industry, and law enforcement and national security agencies. Each party has legitimate concerns and interests. Let me say up front that I believe compromise is necessary. To embrace any one party's concerns to the exclusion of others' will undermine individual liberty or U.S. leadership of the computer industry or our security as a nation, or a combination thereof. Any of these options is unacceptable to the vast majority of the American people.

Current U.S. export policy requires that a key recovery system be built into strong encryption products. The SAFE legislation sponsored by Rep. Goodlatte and co-sponsored by many of you on this Subcommittee, would effectively prohibit the Federal government from mandating a key escrow or key recovery regime. Given SourceFile's unique position as the only firm authorized to provide key recovery

services, you may be surprised by my next comments.


Although my company stands to profit from the government mandate to use key recovery, I am not here necessarily to argue in favor of such a requirement.

Americans are deeply divided over the trade-offs between protecting privacy and property on one hand, and supporting law enforcement officials in the fight against crime on the other. I recently saw an Equifax/Harris poll that shows this division with respect to real time communications. Internet users split 51%–49% on whether "the government needs to be able to scan Internet messages and user communications to prevent fraud and other crimes." Non-Internet users agree 2–1 with that statement (see table).

Table 2

PRIVACY VS. LAW ENFORCEMENT ACCESS TO INTERNET COMMUNICATIONS

“The Government needs to be able to scan internet messages and user communications to prevent fraud and other crimes.”



	Internet Users (Percent)	Non-Internet Users (Percent)
Agree strongly	18	35
Agree somewhat	33	29
Disagree somewhat	25	19
Disagree strongly	24	15

Source: 1986 Equifax/Harris Consumer Privacy Survey, *The Internet*, published in *Inc. Technology*, 1997, No. 1, page 18.

Allowing development and use of encryption strong enough to secure Americans against invasions of privacy and economic espionage while simultaneously allowing for national defense against other forms of espionage and for law enforcement

requires a delicate balancing act. I do not presume to know exactly what policy will provide the balance most Americans seek. But I do know we cannot stand still. We must break this gridlock.

The market is already leading the way, moving toward some sort of key recovery system. And whether the government requires the use of key recovery centers or not, SourceFile will be in the key recovery business because market forces demand our service. Commercial and individual users alike look to key recovery as an essential part of their key management infrastructure, and as a preferred way to secure, manage and control the administration and recovery of encrypted data files.

Encryption users simply will not risk losing access to all their secrets if they lose a key. I have never met a car owner who did not have at least one duplicate key to his car. No one wants to invest in an automobile, lose the key and be unable to open the door. Losing the key for robust encryption is far more disastrous because you cannot call a locksmith to open the door to your data.

Persons who use strong encryption do so to protect extremely valuable assets. No one in his right mind would use cryptography throughout an organization without a backup system to retrieve the information should he lose his key. To repeat, the market will demand key recovery whether government mandates it or not. The only persons who will not avail themselves of a backup system are the foolhardy. Even many criminals will want key recovery.

Concerns about encryption's effects on criminal investigations must be weighed against its benefits in crime prevention. One cannot "lock out" a law enforcement agency's need, with a proper court order, to intercept and decrypt an e-mail; nor should any government entity have a free end to browse and read encrypted communications. As I said at the beginning of my testimony, it is a question of finding the right balance.

For decades, American businesses have sought protection, both privately and from government, against industrial espionage. Today's electronic commerce and flow of digitized data over the Internet make invaluable information vulnerable to industrial espionage unless it is secured with strong encryption.

As the Subcommittee on Crime learned at a hearing last May, the theft of proprietary business information costs American companies from \$24 billion to more than \$100 billion each year.[\(see footnote 1\)](#) That is a wide range. But even if one assumes the lower figure is correct, it still represents an enormous hit on our

nation's economic well being. One good, patented idea may generate hundreds or thousands of new jobs, and lead to the creation of new companies or even an industry. Individuals and companies must be able to safeguard proprietary information against determined economic espionage efforts.

My firm, SourceFile, is an international leader in protecting intellectual property. Hundreds of developers and user organizations from more than 20 countries rely on SourceFile to hold their program source code in escrow. As a trusted third party, SourceFile's parent company hold millions of highly confidential corporate and financial records, hospital records, and, perhaps most sensitive of all, records from AIDS tests. I mention this to make two points. First, there is precedent for third parties that are properly equipped, secured, and insured to be trusted with the most confidential information imaginable. Second, SourceFile and companies like it are bound by strict laws that protect the privacy of the persons whose records we hold. There should be and are severe penalties if a third party breaches the trust reposed in it.

SourceFile believes that the protection of private property rights dictates that severe penalties should be levied against key recovery centers that abuse the trust placed in them. Such penalties would be similar to those for banks that misappropriate or embezzle depositors' funds.

In the new information age, intellectual property is many companies' most valuable asset. For example, one of our clients designs and develops gene sequence and expression databases. Their revenue comes from leasing access to these databases. If anyone broke their encryption and stole their databases, the company's asset and market values would plummet. The means to transfer data securely is essential to this firm and a fast-growing number of others like it. Most of these firms, I might add are American and represent an important new source of employment and economic prosperity for our country.

These companies will benefit now, if they can use strong encryption worldwide. The uncertainty over what policy and what law will govern their actions inhibits them from using robust encryption.

I believe the companies who are our customers want and expect government to help them protect their intellectual property and trade secrets through vigorous law

enforcement. I further believe our customers recognize there will be occasions when law enforcement will require access to encrypted data.

But for government to restrict the strength of encryption that these new information-based companies can use will either make them vulnerable to theft of their intellectual property or drive them offshore. Either way, it is an untenable policy for the United States as we move into the information age.

A graduate student at the University of California at Berkeley named Ian Goldberg proved in January that stronger encryption is needed. According to news reports, it took Mr. Goldberg only 3 1/2 hours to break the most secure encryption code the United States allows to be freely exported. He did so by linking together 250 idle workstations that allowed him to test 100 billion possible "keys" per hour. As far as I know, Mr. Goldberg is not a criminal of any sort. But if a lone graduate student could marshal the computing power to break this encryption, you can be certain that a foreign intelligence service, or a large corporation or even a technologically-savvy thief can do so, too.

Certainly it makes sense to maintain export controls on hardware and software for military applications as the SAFE bill does. But any attempt by government to hold back the progress of encryption technology will be futile. Microprocessor technology is advancing relentlessly. Encryption will rapidly continue to get stronger and stronger, whether it is produced in the United States or elsewhere. Even if government succeeds in retarding improvements in encryption used by law-abiding persons, those seriously determined to break the law will find sources for the strong encryption and code-breaking products they desire.

Rather than attempt to hold back the hands of time or put the Genie back into the bottle, it makes more sense to levy criminal penalties against those who use cryptography to commit a crime. The SAFE bill would do that.

Finally, we believe it is reasonable to expect key recovery centers to comply with law enforcement authorities who, through due process, present court orders for access to encryption keys. Such cooperation is analogous to telephone companies who permit officials with proper legal authorization to install wiretaps. Following this analogy, key recovery centers who obey court orders should not be liable to civil penalties for such compliance.

Mr. Chairman, I thank you and the other Members of this Subcommittee for the privilege to appear before you and for your attention. I will be pleased to answer

your questions.

[\(Footnote 1 return\)](#)

Transcript of Hearing on Economic Espionage conducted by the Subcommittee on Crime, House of Representatives, May 9, 1996, pp. 1 and 59.

**NATIONAL
SECURITY
ARCHIVE**

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu