

# THE PRIVACY PAPERS

Number 4

November  
1998

## Cypherpunks vs. Cryptocrats: The Battle Over the U.S. Encryption Standard

By Lisa S. Dean

Free Congress  
Foundation

Within the last decade, America and the rest of the world have become wholly dependent upon computers and other emerging technologies to conduct business and communicate. The current trend suggests that this dependency will increase with time rather than decrease, as some have suggested.

This technology, not unlike traditional communications tools, is amoral in itself. It can be used to benefit businesses and families but is also subject to various uses and abuses by those who wield it as a weapon in an attempt to advance a particular agenda.

One key new issue related to technology is encryption, a system which scrambles electronic information such as computer files, email, telephone conversations, fax data and countless other transactions or transmissions sent through electronic means. When someone sends an encrypted message, he uses two unique keys. The private key is used to scramble the message while the public key is sent out to the intended recipient so he can "unlock" or decode the contents of the message.

Various forms of encryption have been used for centuries. However, in his book *The Codebreakers*, David Kahn contends that while people have long been communicating in code for centuries, the use of encryption technology did not really begin until World War I.<sup>1</sup> Further, the military was the only entity that used such technology.

For that reason, encryption was classified as a munition; therefore, its export was restricted. Now, with the dawn of the Information Age, over 189 million computer users worldwide are clamoring for security for their documents and electronic transmissions. Many nations, including the Scandinavian countries, Japan, and Australia, have permitted the use of strong encryption (233-bit and up) among their citizens, thereby encouraging the use of electronic commerce and communications. However, the same cannot be said for the United States. The Clinton Administration, since its inception, has forbidden American software manufacturers and individual cryptographers from export encryption stronger than 56-bit without making it "key recoverable," that is to say, without leaving the public key that would decode the information on file with government agencies.

There are several problems with this policy. First, because of the time and cost required to develop encryption systems which then cannot be exported, export restrictions are a disincentive to companies and independent cryptographers to develop strong encryption algorithms at all. It would be an understatement to call this situation a sad one. Traditionally, it has been US technology that has paved the way for foreign countries and companies. Now we must surrender our lead to others.

Worse, we are exporting our research and development skills instead of our products. Students from foreign countries enter American universities and learn how to create strong encryption algorithms, only to return to their own countries to develop them into

---

<sup>1</sup> Kahn, David. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. (New York: Scribner, 1996.) This volume was first published in 1967 as one of the most comprehensive histories and explanations of cryptology, when the subject itself was not yet an issue, even among the cypher community. Today the book is still considered the most comprehensive explanation of the subject.

actual software products. The US is training the citizens of foreign countries to develop strong encryption, which will be used to protect their own information, including, by their governments, for missiles, weapons of mass destruction and other national security programs.

It is mostly students from India, China and other nations which have traditionally not been allied with the US that are benefiting from this knowledge and know-how. It seems contradictory of the Administration to allow the export of this knowledge to foreigners, but at the same time to forbid American mathematicians and computer scientists from exporting their products. The US software industry reports losing tens of millions of dollars each year as a result of Clinton's export restrictions.

A second problem with the Administration's mandate of "no exports" is that no software containing encryption stronger than 56-bit may be exported from the US without a "back door" or "key" to allow federal law enforcement easy access to and retrieval of the encrypted information.

In a study produced by an ad hoc group of cryptographers and computer scientists in 1996, the fragility of a 56-bit encryption code was demonstrated. They estimated that it would take a large corporation approximately six minutes and a government intelligence agency 12 seconds to crack such a code.<sup>2</sup> In other words, a 56-bit encryption code buys you 12 seconds of security. The Electronic Frontier Foundation built a computer using "off-the-shelf" technology that cracked a 56-bit encryption code in three days. Once again, this illustrates the lack of true security that the government standard provides.

During Clinton's first term, "key recovery" was introduced as part of a proposal by the Administration known as the "Clipper Chip" proposal. When Clipper was first introduced in Congress, it was soundly rejected without much debate. Then came two additional attempts known as Clipper II and Clipper III, both of which suffered the same fate.

Having tried unsuccessfully at the legislative level, David Aaron, President Clinton's ambassador on this project, lobbied the 27-member Organization for Economic Cooperation and Development (OECD) to consider and eventually adopt such a requirement at the international level. After serious consideration, the OECD sent a detailed letter to all member nations issuing a stern warning against adoption of such a system on the grounds that it would be a direct and blatant violation of citizens' privacy. Nevertheless, the Administration has consistently maintained that "key recovery" is favored by nations across the globe.

Interestingly, in 1997 the Global Internet Liberty Campaign conducted a survey of 230 nations asking their national security advisors if they would consider such a system. Of the 225 nations that responded, only eight agreed that such a system would likely be adopted in their countries. Those nations were China, France, India, Israel, Pakistan,

---

<sup>2</sup> The report is entitled "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security" and copies can be obtained through the National Research Council.

Republic of Korea, Russia, and Singapore.<sup>3</sup> It is of interest that only eight nations agreed to adopt such a system, but what is even more telling is that, with the exception of France, Israel and India, none of the nations accepting key recovery have a strong democratic tradition.

The final result here in America is that no strong encryption exists to prevent hackers, other online miscreants or the government from intercepting confidential or personal information such as bank records, personal communications and other material unintended for prying eyes. While the Administration's position has been that encryption can be developed within the country but cannot be exported, it has also considered the posting of encryption algorithms on the Internet and "disclosing" such information to foreigners to be in violation of US export laws.

### Legal cases

The Administration's position has led to a number of court battles, such as *Zimmerman vs. US Department of State*, *Karn vs. US Department of State*, *Junger vs. US. Department of State* and the most recent, *Bernstein vs. US Department of State*, which is still being decided in the US Court of Appeals for the Ninth Circuit.<sup>4</sup>

All of these cases are similar in the sense that the basis for each case is First Amendment rights. However, the details in each are worth mentioning for the purpose of illustrating the lengths to which the Clinton Administration has gone and will go in order to prevent encryption from being exported.

*Karn vs. US Department of State*: Phil Karn was a computer programmer who requested permission from the US State Department to export Bruce Schneier's *Applied Cryptography* textbook in physical book form. He was granted permission to do so. Karn then requested permission to export that same book in disk format and was denied such a request. The State Department argued that the appendices of that book contained source code for strong encryption algorithms, such as Pretty Good Privacy (PGP), and could be executable if received in disk form, a violation of US export law. Karn argued that the Administration's policy was inconsistent with that law. The lower court ruled in favor of the Administration and the Karn case is currently awaiting a decision on appeal.

*Zimmerman vs. US Department of State*: Phil Zimmerman was accused by the Administration of violating export laws by posting Pretty Good Privacy (PGP), his own encryption algorithm, on the Internet. While Zimmerman developed PGP, he denied ever having posted it on the Internet. The US Customs Agency convened a grand jury to determine whether Zimmerman actually posted his algorithm in violation of US export laws. Zimmerman was never indicted by the grand jury, which could not gather enough evidence to bring criminal charges. Earlier this year, Zimmerman published his

---

<sup>3</sup> The report, entitled "Cryptography and Liberty: An International Survey of Encryption Policy" can be found at the Global Internet Liberty Campaign's website at [www.gilc.org](http://www.gilc.org).

<sup>4</sup> For more detailed information on each of these cases, please contact the Electronic Frontier Foundation's website at [www.eff.org](http://www.eff.org). There you will find a detailed summary of each case and how it has effectively impacted US export law.

algorithm in book form rather than on disk and shipped it to a company in Denmark, which scanned it in page by page and created the algorithm electronically for worldwide distribution. The objective was to prove the absurdity of the Clinton Administration's position on export controls.

*Bernstein vs. US Department of State:* Daniel Bernstein, at the time a graduate student in mathematics at the University of California at Berkeley, also posted his encryption algorithm on the Internet, for the purpose of generating discussion among his colleagues. When the Administration came in and demanded that he remove it for violating federal export laws, Bernstein applied for an export license. After years of waiting, he was finally rejected and turned to the courts to settle the matter. Bernstein won his initial case against the Administration and the judge sternly warned the Administration to change its export policy. Instead of heeding the judge's advice, the Administration appealed and lost once again. The case is now on its second appeal in the US Court of Appeals for the Ninth Circuit and is awaiting a decision.

*Junger vs. US Department of State:* A case was made by the Administration that export laws were being violated because Peter Junger, a law professor at Case Western Reserve University, was teaching a class in computer law and cryptography was a detailed part of the course. Because foreign students were part of the class and because Junger had colleagues who were foreign nationals, it presented a complicated situation relative to the Administration's restrictions on "disclosing encryption information to foreigners." Professor Junger brought suit against the Administration, arguing that his First Amendment rights were violated because the Administration limited his freedom of expression without first detailing clearly defined standards. It is important to note that there is no law which currently prohibits a university, private or public, from permitting a foreign student to attend a class where encryption is discussed or one in which the formulation of its algorithms are taught. Like Karn, Junger lost at the lower court and has appealed to the Sixth Circuit, which is awaiting the Bernstein decision from the Ninth Circuit before scheduling the case for trial.

### Legislative measures

#### **SAFE Act:**

While some have battled the issue in the courts, others have taken the legislative route to either support or oppose the Administration's restrictions. As stated previously, from its inception, the Clinton Administration has been pushing for a legislative measure that would reflect its policy on encryption. Until 1997, all legislative attempts were failures. However, with FBI Director Louis Freeh as his top lobbyist on Capitol Hill, Clinton has managed to gain considerable ground on the legislative battlefield.

In early 1997, Representative Bob Goodlatte (R-VA) introduced his Security and Freedom through Encryption Act (SAFE) as an alternative to the Administration's regulations regarding encryption exports. While SAFE received widespread support in Congress and was hailed as a breakthrough in protecting the Constitutional rights of

citizens by not forcing Americans to turn over the keys to their computers to a federal agency, it was not the answer for many critics of the Administration's policy.

SAFE proposed measures to allow hi-tech companies to manufacture and distribute encryption domestically regardless of key length or strength. It would also ease (not remove entirely) export restrictions by allowing US manufacturers to export their encryption products provided that the same strength is already available on the market from a foreign competitor. Finally, SAFE imposed a stiff penalty on people who used encryption during the commission of a crime.

While those provisions may have sounded reasonable to most Congressmen, some Senators and even some hi-tech companies (who wanted a reasonable compromise for fear of losing even more money if the Administration continued its export restrictions), it was deemed unacceptable by most cryptographers and privacy advocates for a number of reasons.

First, while domestic controls on encryption appeared to be lifted entirely in this bill, the reality was that a provision within it allowed for the government to dictate to industry if and when they wanted key recovery features added to a company's products.

Second, while the bill allows the exportation of a US encryption product when the same product is available through a foreign competitor, it is not a solution to tell US manufacturers that, while they have traditionally been in the lead in computer technology and especially encryption technology, they now have to remain on a par with their foreign competition.

Finally, adding a criminal penalty for the use of encryption in the commission of a crime is nothing short of ludicrous. The principle behind such a measure is to dissuade criminals from using encryption. Anyone with an elementary understanding of the criminal mind knows that a drug lord, for example, is not going to avoid using encryption to cover his tracks simply because it breaks another law. Gun laws offer a similar case. Drug lords still use guns in the commission of their crimes, but upstanding citizens now have to register their weapons with the government.

The same will hold true for encryption, which is why it is fair to label "key recovery" encryption as gun control for the Information Age. While criminals continue their crimes, using encryption to secure their information, upstanding citizens will be forced to hand the keys to their computers over to the government, making their personal information subject to the curiosity of government agents.

**Oxley/Manton Amendment:**

An amendment to SAFE was introduced by Representatives Mike Oxley (R-OH) and Tom Manton (D-NY) that essentially made a weak bill weaker by imposing stronger restrictions on the domestic use of encryption. In a nutshell, Oxley/Manton reinserted "key recovery" provisions into SAFE, requiring citizens to keep the keys to their computers on file with the federal government.

While the SAFE Act, complete with the Oxley/Manton Amendment, was reviewed by several House committees, it was not voted on in the last Congress.

### **Secure Public Networks Act of 1997:**

Quite possibly the most dangerous piece of legislation in the Congress today, S. 909, the Secure Public Networks Act of 1997, was introduced by Senators John McCain (R-AZ) and Bob Kerrey (D-NE). It is practically identical to President Clinton's Clipper III proposal. Its intention was to combat identity theft on the Internet, but it actually sets up a massive "key recovery" program here in the US.

Through a Key Management Infrastructure (KMI), the Act would establish a nationwide system of agencies known as Certificate Authorities that would register citizens' digital signatures to prevent fraudulent use of identities. The result would be that the federal government would keep on file the "identities" of every American who uses a computer or other electronic means of communication. In addition, the Act requires that anyone who receives federal funds for their networks and any encryption product used by the government must use a key recovery system. This includes universities, public schools, the banking industry and a major portion of the commercial sector of society.

While the bill was reported to the Senate, it was not voted on in the last Congress. However, sentiment among Senators is that a vote will likely take place in the 106<sup>th</sup> Congress.

### **E-PRIVACY:**

In May of 1998, Senators John Ashcroft (R-MO) and Patrick Leahy (D-VT) introduced what they called their answer to the Secure Public Networks Act of 1997, Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY). While the original version of E-PRIVACY was weak, the latest version is much stronger and more reflective of the views of Constitutional scholars and privacy advocates rather than industry and government officials. The bill's revision is largely due to the dissatisfaction expressed by privacy-oriented organizations. While still being revised, E-PRIVACY protects the rights of all Americans to use the strongest encryption available without being forced to turn over their keys to the federal government. Further, it eliminates export controls on encryption, not only for the software manufacturer in Silicon Valley, but also for the individual cryptographer who wants to post his algorithm on the Internet or to export it through other means. Currently, E-PRIVACY is the only piece of legislation in either House of Congress that eliminates export controls on encryption.

In addition to containing no "key recovery" provision, the bill also assumes that criminals will use whatever tools available to commit crimes. That being the case, the criminal ought to be punished for the crime itself, rather than the means he used to commit it. Therefore, the criminal provision in SAFE does not exist in E-PRIVACY.

E-PRIVACY is thus far the strongest measure in Congress to protect citizens' Constitutional rights. While the measure is expected to be reintroduced in early 1999,

much opposition is anticipated from the White House and Members of Congress who contend that all citizens must give the government access to their electronic information despite the fact that in so doing they relinquish their Fourth Amendment rights to protection from unreasonable searches and seizures.

**Conclusion:**

Sadly, we have reached a stage in our country where we are faced with a battle for the protection of our Constitutional rights. This battle is waged, not by our foreign enemies, but by our own government, our own president and Congress who swore to uphold and defend the Constitution of the United States.

Those same people are today calling the Constitution "an evolving document," one that changes with the times. FBI Director Louis Freeh stated before the US Senate that "we need a Fourth Amendment for the Information Age." That belief, combined with our Constitution not being taught any longer even in law schools, has led to an ignorance of the Constitutional crisis we are in today. How can people preserve their rights if they don't know they have them? The answer is, they cannot and they are not. That has made the job of eroding the Constitution as the supreme law of the land such an easy task.

As we move deeper into the Information Age, our use of technology will become second nature to all of us, whether we use a computer or not. As author C. S. Lewis stated, "The pain now is part of the happiness later." The stance we take now will forever affect how future generations live. It is up to us to decide their fate and ours and we have no time but now in which to do it.