The Legal Report

Denning to Leahy: Don't Eliminate U.S. Crypto Export Controls

---

Richard L. Field
Contributing Editor, JIBC Legal
field@pipeline.com

Richard Field is an attorney and legal consultant in Cliffside Park, New Jersey, U.S.A. He chairs the Electronic Commerce Payment Committee of the American Bar Association, and is a drafter of the forthcoming Digital Signature Guidelines of the ABA Information Security Committee.

On March 5, 1996, Senator Patrick Leahy (Vermont) introduced S. 1587, the Encrypted Communications Privacy Act of 1996, in the U.S. Senate. Leahy said his legislation was intended to protect government, business and home computer users from outside snooping into sensitive information. He said the new law was written to encourage the use of encryption and loosen export restrictions on encryption technology. Senator Leahy's press release page is at: http://www.senate.gov/~leahy/p960305.html

Reaction to the bill within the U.S. cryptography community has been mixed. Some have applauded Senator Leahy's stand on loosening cryptographic export restrictions. At the same time, a provision criminalizing the use of cryptography, when used in the commission of a separate crime, has caused concern. As of this writing, the future of the bill is uncertain.

Professor Dorothy Denning, a recognized expert in the field, submitted her own views to Senator Leahy by means of a letter responding to the bill. I thought it would be useful to reprint her position on this important issue, which I do here with permission.

March 14, 1996

The Honorable Patrick Leahy
United States Senate
Russell Building, Room 433
1st and C Streets, NE
Washington, DC 20510

Dear Senator Leahy:

As author, scholar, lecturer, researcher, and consultant to the government and industry in cryptography and information security, I am concerned that S.1587, the "Encrypted Communications Privacy Act of 1996," is not in balance with society's needs. By removing practically all export controls on encryption, the bill will make it far easier for criminals, terrorists, and foreign adversaries to obtain and use encryption that is impenetrable by our government. The likely effect will be to erode the ability of our law enforcement and intelligence agencies to carry out their missions. This is not consistent with your own findings in the bill which recognize the need for a "national encryption policy that advances the development of the national and global information infrastructure, and preserves Americans' right to privacy and the Nation's public safety and national security."

I am concerned that the proposed legislation responds only to a loud cry for assistance and is not the reasoned and practiced position of our multinational corporations. At the International Cryptography Institute, which I chaired in September 1994 and 1995, our discussions did not find that this unrestricted distribution of encryption technology was

required to satisfy business objectives. Our corporations recognize the need to respect the legitimate interests of governments and the need for encryption methods that use "key escrow" or "trusted third parties" with data recovery capabilities to protect their own information assets. Businesses are moving in the direction of key escrow, and key escrow is becoming a standard feature of commercial products. I have recently summarized the features of thirty products and proposals for key escrow in a taxonomy which I developed with Dennis Branstad.

Because of the need to address information security at an international level, the Organization for Economic Cooperation Development, through its Committee for Information, Computer, and Communications Policy, is bringing together the international business community and member governments to develop encryption policy guidelines that would respect the interests of businesses, individuals, and governments. In support of that objective, the INFOSEC Business Advisory Group (IBAG), an association of associations representing the information security interests of users, issued a statement of principles recognizing the needs of governments, industry, and individuals, and supporting approaches based on trusted third parties. A similar statement was issued by a quadripartite group consisting of EUROBIT (European Association of Manufacturers of Business Machines and Information Technology Industry), ITAC (Information Technology industry Association of Canada), ITI (Information Technology Industry Council, U.S.), and JEIDA (Japan Electronic Industry Development Association), which accounts for more than 90% of the worldwide revenue in information technology. X/Open is pursuing a public key infrastructure project aimed at creating specifications and possibly operating manuals that could be used in conformance testing and site accreditation of trusted parties.

The European Commission has proposed a project to establish a European-wide network of trusted parties that would be accredited to offer services that support digital signatures, notarization, confidentiality, and data integrity. The trust centers, which would be under the control of member nations, would hold keys that would enable them to assist the owners of data with emergency decryption or supply keys to their national authorities on production of a legal warrant.

Within the U.S., the Clinton Administration is developing federal standards for key escrow encryption (these are in addition to and more general than the original Clipper standard, FIPS 185), adopting escrowed encryption within the federal government, and liberalizing export controls on encryption products that include an acceptable system of key escrow. The Administration's policy has considerable flexibility, allowing for both hardware and software implementations, classified and unclassified algorithms, and government and private sector key holders. Some companies have submitted products for review under the liberalized export controls for key escrow encryption. Trusted Information Systems has already received approval for their Gauntlet firewall.

Industry is also developing cryptographic application programming interfaces (CAPIs), which will facilitate the inclusion of cryptographic services in applications, networks, and operating systems. This approach, recently demonstrated by Microsoft, will allow U.S. software companies to develop exportable applications and systems that run with separate security modules. These modules can provide either domestic grade encryption or exportable encryption. The impact of export controls will thus be limited to those companies selling encryption modules, not the entire U.S. hardware and software industry. Even this impact can be made negligible by allowing companies to export security modules with strong encryption where the keys are held with escrow agents in the purchaser's country. Bilateral mutual assistance agreements could ensure that U.S. law enforcement agencies are able to obtain decryption assistance if the exported module is used in a crime against the U.S. CAPIs are providing the technological base for experiments under the International Cryptography Experiment (ICE), an informal international alliance of individuals and organizations working together to promote the international use of encryption within import and export regulations that respect law enforcement and national security interests.

As these examples illustrate, businesses and governments are working hard to establish policies and technologies that respect the needs of users, industry, and governments in the furtherance of a secure global information infrastructure. Considerable progress has been made during the past year. The export provisions in S.1587 are likely to undermine those efforts by satisfying the immediate export demands of a few U.S. companies at the expense of other stakeholders and society at large. It will undermine the ability of governments worldwide to fight global organized crime and terrorism.

Although some U.S. companies have lost sales because of export controls on encryption, the overall impact of these

controls on the U.S. information technology industry as a whole is much less clear. In the most comprehensive study of export controls to date, the Department of Commerce and National Security Agency found that in all but three countries surveyed, sources indicated that U.S. market share (about 75% overall) was keeping pace with overall demand. Most of the impact was found to be on the sale of security-specific products, which account for only a small percentage of the total market, rather than general-purpose software products. Sales of security-specific products are generally few and mostly to customers within the country where the product originates. Visits to 50 computer and software stores in Canada, France, Germany, Japan, S. Korea, Thailand, and the U.K. found that all the general-purpose software products with encryption were from U.S. manufacturers. The study concluded that "the impact of U.S. export controls on the international market shares of general-purpose products is probably negligible" and that "the export licensing process itself is not a major obstacle to U.S. competitiveness." This is in stark contrast to the dire prediction of the Computer Systems Policy Project that U.S. industry stands to lose $30-60 billion in revenues by the year 2000 because of export controls.

The Commerce/NSA study did acknowledge that the existence of foreign products claiming strong encryption could have a negative effect on U.S. competitiveness. However, by allowing encryption services to be sold separately from the applications software that uses them, CAPIs will make it extremely unlikely that general-purpose software will be substantially effected by export controls. Even security-specific products, which are a growing industry, can use CAPIs to separate out the encryption component from the main product (e.g., firewall). Moreover, if keys can be held in other countries under appropriate bilateral agreements as noted earlier, export controls need not substantially impact encryption products.

Export controls are often blamed for the lack of security in our public infrastructure. The Commerce/NSA study found "little evidence that U.S. export controls have had a negative effect on the availability of products in the U.S. marketplace," although they "may have hindered incorporation of strong encryption algorithms in some domestic mass-market, general-purpose products." There are many factors which have played an even larger role in the general lack of security we find on the Internet: the high cost and low demand for security, the difficulty of designing systems that are secure, pressure to bring new products to market before their security implications are understood, the willingness of users to take risks in favor of acquiring new tools and services, and lack of a public key infrastructure to support encryption on a national and international basis. Many systems are so riddled with security holes that any would-be attacker can gain access to the system itself, and from there access to plaintext data and keys. Malicious code can be injected into a victim's system through electronic mail, documents, images, and web browsers; once there, it can transmit sensitive data back to its owner. Keyboard sniffers can capture a user's keystrokes before they are ever encrypted. Thus, while export controls have played a part in the slow integration of strong encryption into software and systems, they are not responsible for most of the security vulnerabilities we see today. Moreover, most of these vulnerabilities are remedied with non-cryptographic controls (e.g., process confinement, trusted systems engineering, biometrics, and location-based authentication) or with cryptographic techniques for authentication, data integrity, and non-repudiation, which are exempt from State Department export controls. I do not mean to suggest that encryption is not important. In fact, it is essential to protect against certain threats. However, it must be kept in perspective. The use of encryption for confidentiality protection is but one small, albeit important, piece of an information security program.

The provisions is S.1587 regarding trusted key holders could have the benefit of increasing public trust in key holders. However, I have some concern that the current provisions may be overly restrictive. Thus far, we have practically no experience with the operation of third party key holders and the circumstances under which they will be called upon to provide keys or decryption assistance. It will be extremely important that the provisions allow enough flexibility to accommodate legitimate use of the data recovery services of key holders for criminal investigations, civil litigation, and intelligence operations. The liability risks to key holders should not be onerous. The definition of key holder and exact wording in the bill may also need some refinement in order to accommodate existing and proposed methods of trusted third party encryption.

Encryption policy is a difficult and often emotional issue. It is important that Congress work closely with the Administration, industry, and other interested parties to develop the best legislative strategy for promoting information security on the national and global information infrastructure without diminishing the ability of our law enforcement and intelligence agencies to protect the public safety and national security. Export liberalization should proceed cautiously, tied to key escrow or other methods that accommodate the needs of the government as well as those of

users and industry. The Administration's plans to liberalize export controls on software key escrow is a good next step. As trust and confidence in key escrow grows, the export of virtually unlimited strength encryption systems may be possible. Because export controls are our only lever for controlling the spread of encryption, they should be used to their full advantage. Decisions to liberalize these controls must be fully informed by classified national security information as well as by economic analysis and market studies.

Law enforcement agencies are encountering encryption with ever greater frequency. Within a few years, the successful execution of practically all court-ordered intercepts and searches and seizures is likely to depend on their ability to decrypt communications and stored information. If the encryption cannot be broken, it could be impossible to successfully investigate or prosecute those cases. Crimes of terrorism and white collar crime, including fraud, embezzlement, and money laundering, would be facilitated and perhaps impossible to solve. Even crimes of economic espionage, which often involve insiders with access to company secrets, are facilitated with encryption. It will be important for Congress to closely monitor the impact of encryption on law enforcement and use that information to guide any encryption legislation.

In summary, our national policy can and must promote the legitimate use of strong encryption for information protection without unnecessarily hindering the ability of our law enforcement and intelligence agencies to do their jobs. In so doing, the policy can accommodate reasonable liberalization of export controls and business objectives without undermining other national objectives. Such a policy is consistent with your own guiding principle for the bill: "Encryption is good for American business and good business for Americans." But it goes further in order to be equally guided by the principle that law and order and national security are essential for the American economy and the American people. It is not necessary to so radically lift export controls on encryption in order to accommodate both principles.

I will be pleased to meet with you and the committee for comment and questioning, or to assist in any way I can with the development of a balanced approach to encryption legislation.

Yours respectfully,
Dr. Dorothy E. Denning
Professor of Computer Sciences
Georgetown University
denning@cs.georgetown.edu
http://www.cosc.georgetown.edu/~denning