KENNETH W. DAM
HERBERT S. LIN

National Cryptography Policy for the Information Age

Relaxing federal regulation will lead to enhanced information security for all.

Accelerating growth in the use of information technologies to store and communicate digital data is creating a parallel need for measures to ensure the security of this information. Unfortunately, in the critical area of cryptography (the use of mathematical formulas to scramble information into digital codes), government policy is not keeping pace with developments in the market and the technology. In fact, current federal regulations actually discourage the foreign and domestic use of this important technology.

U.S. export control laws limit the sale of strong encryption products overseas in the interest of denying to foreign countries the ability to encode information in ways that would make it more difficult for U.S. authorities to gain access to that information for national security and foreign policy uses. However, these controls also impede the efforts of U.S. companies with foreign customers and suppliers to protect their proprietary business information, and they constitute a barrier for U.S. information technology vendors who wish to market their products to security-conscious foreign buyers. Export controls also reduce the domestic availability of strong encryption because they drive many U.S. vendors to a "least common denominator" strategy of product development, marketing, and support that calls for a single and relatively weak product that can be sold domestically and abroad.

More recently, the Clinton administration has aggressively promoted the domestic use of escrowed encryption, a form of cryptography in which a copy of the key needed to decode data is stored in an ostensibly safe place by a third party. Escrowed encryption is intended to provide strong protection for legitimate uses but also to enable law enforcement officials to gain legally authorized access to the encryption key when it is necessary to decode data as part of a criminal investigation. However, many businesses and individuals do not see the value in using escrowed encryption because dependence on a government-approved product is likely to slow innova-

Kenneth W. Dam is Max Pam Professor of Law at the University of Chicago and was deputy secretary of state from 1982-1985. He chaired the National Research Council's Committee to Study National Cryptography Policy, which produced the report *Cryptography's Role in Securing the Information Society* (National Academy Press, 1996). Herbert S. Lin was study director for the committee.

tion, and they worry about the security of the extra copy of the decryption key.

What is lacking in federal policy is a market-sensitive understanding that information security is a critical concern for all sectors of society, not just the government. Businesses, especially those operating internationally, must share sensitive information with certain customers, suppliers, and strategic partners while protecting that information against competitors, criminals, foreign governments, and other suppliers and customers. Private citizens conduct sensitive conversations over cellular and cordless telephones that are easily overheard. A rapidly growing number of business and personal financial transactions are now conducted electronically. These private sector interests parallel those of the federal government in ensuring that its important and sensitive political, economic, law enforcement, and military information, both classified and unclassified, is protected from foreign governments and hostile parties.

A false dichotomy

The problem for policymakers is that cryptography that is available to the general public for legitimate uses is also available for illegitimate purposes such as organized crime and terrorism. Encryption thus could make it more difficult for law enforcement authorities to gain legally authorized access to information for the purpose of investigating and prosecuting criminal activity. Encryption also poses a threat to intelligence gathering, which depends on access to information from foreign governments and other foreign entities; such intelligence is valuable for national security and foreign policy purposes

But information gathering, which would unquestionably be hindered by encryption, is a tool, not the ultimate goal of law enforcement and national security. The widespread use of cryptography would advance many of the larger interests of law enforcement and national security. If encryption can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can), the job of law enforcement becomes easier. If encryption can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports national security. If cryptography can ensure confidentiality, provide reliable user authentication, and detect unauthorized tampering with electronic data in individual consumer transactions (which it can), it can help deter electronic bank fraud and many other types of illegal activity, thereby reducing crime and enabling law enforcement authorities to focus their limited resources more effectively.

Thus, it is a false dichotomy to characterize the debate over national cryptography policy as a trade-off between the government's interests in law enforcement and national security and the nongovernment information security needs of businesses and individuals. Recognizing this broader context more explicitly would go a long way toward reducing the counterproductive polarization that has too often characterized the national debate. Informed public discussion of the issues must begin with all stakeholders acknowledging the legitimacy of several goals: information gathering for law enforcement and national security purposes and information security for law-abiding individuals and businesses.

A second barrier to constructive discussion of cryptography policy deserves attention. Effective debate has often been stymied by claims that decisions on national cryptography policy depend on classified information that cannot be shared with the public. Thirteen of the 16 members of the National Research Council's Committee to Study National Cryptography Policy received security clearances to examine this classified information. They concluded that although classified information is often important to operational decisions in specific cases, it is not essential for crafting policy or understanding how the technology will evolve.

Framework for a new policy

Because cryptography is an important tool for protecting information and because it is very difficult for governments to control, policymakers must recognize that the widespread nongovernment use of cryptography in the United States and abroad is inevitable in the long run. The proper role of national cryptography policy, therefore, is to facilitate a judicious transition from today's world of information vulnerability to a future world of information security, while meeting to the extent possible the legitimate needs of law enforcement, national security, and foreign policy. U.S. cryptography policy should be built on three principles:

- The broad availability of cryptography to all legitimate elements of U.S. society;
- Continued economic growth and leadership of key U.S. industries and businesses in an increasingly global economy, including but not limited to U.S. computer, software, and communications companies;
- Public safety and protection against foreign and domestic threats.

The first two objectives argue for a policy that places few government restrictions on the use of cryptography and actively promotes the use of cryptography on a broad front. The third argues for some kind of government policy role in the deployment and use of cryptography.

One aspect of federal policy that is slowing progress in the use of cryptography is the uncertainty it creates for vendors and potential users. Users are reluctant to take actions that might be made obsolete by subsequent policy decisions. For example, businesses are unlikely to purchase products with sophisticated encryption capabilities when it is possible that government will later mandate or unduly favor the use of an incompatible product. As a first step, policymakers should set some clear boundaries on the reach of federal regulations and establish a coherent structure for policy development that ensures that the needs of nongovernment cryptography users are respected. Specifically:

No law should bar the manufacture, sale, or use of any form of encryption within the United States. The administration has wisely rejected the option of banning unescrowed encryption. Such a ban would be easily circumvented technically and would also raise a number of constitutional issues whose outcome is highly uncertain.

National cryptography policy should be developed by the executive and legislative branches on the basis of open public discussion and should be governed by the rule of law. Only a national discussion of the issues involved in national cryptography policy can result in the broadly acceptable social consensus that is necessary for any policy in this area to succeed. A consensus derived from such deliberations, backed by explicit legislation when necessary, will lead to greater public acceptance and trust, a more certain planning environment, and better connections between policymakers and the private sector.

No law should bar the manufacture, sale, or use of any form of encryption within the United States.

National policy affecting the development and use of commercial cryptography should be more closely aligned with market forces. As cryptography has assumed greater importance to nongovernment interests, national cryptography policy has become increasingly disconnected from market reality and the needs of parties in the private sector. To harness market forces to promote widespread use of cryptography, federal policy should emphasize the freedom of domestic users to determine cryptographic functionality, protection, and implementation according to their security needs as they see fit; encourage the adoption of cryptographic standards by the federal government and private parties that are consistent with prevailing industry practice; and support the use of algorithms, product designs, and product applications that are open to public scrutiny. For example, the administration has argued that escrowed encryption would benefit private users by making it possible to recover encrypted stored data to which access has been inadvertently lost. To the extent that this is true, market forces should be sufficient to generate a growing market for products that provide escrowed encryption services for stored data, and aggressive government promotion of this particular application is not necessary.

Today, U.S. firms compete and operate in a global market. Many U.S. firms have close relationships with foreign suppliers, customers, and strategic partners. Under such circumstances, a U.S. firm will inevitably need to share some of its sensitive or proprietary information with these parties, and protecting this information abroad is as necessary as protecting it within the United States. Some relaxation of today's export controls on cryptography is warranted. Relaxation would create an environment in which U.S. and multinational firms could use the same security products everywhere, thereby supporting better information security for U.S. firms operating inter-

nationally. And by expanding the market for cryptography products, it would create an incentive to develop better technology.

Looking to the future, the nation must recognize that foreign companies have the capability to integrate high-quality cryptographic features into their products and services. U.S. export controls will not prevent foreign firms from gaining access to advanced cryptography, and foreign competition may well develop to fill the void created by the absence of U.S. vendors in this market. Such development would be detrimental to U.S. national security interests, as well as to U.S. business and industry. Conversely, relaxation of the controls would help to solidify U.S. leadership in a field critical to national security and economic competitiveness.

At the same time, cryptography is inherently dual-use in character, with important applications to civilian and military purposes. The retention of some export controls on cryptography will mitigate the loss to U.S. national security interests in the short term, allow the United States to evaluate the impact of relaxation on national security interests before making further changes, and buy time for U.S. national security authorities to adjust to a new security environment.

The export control regime in cryptography should be progressively relaxed but not eliminated in the following ways:

Products providing confidentiality at a level that meets most general commercial requirements should be easily exportable. Today, products with encryption capabilities that incorporate the 56-bit DES algorithm provide this level of confidentiality and should be easily exportable. As a condition of export, vendors of products covered under this recommendation would be required to provide the U.S. government with the full technical specifications of their product and reasonable technical assistance upon request, in order to assist the U.S. government in understanding the product's internal operations. This requirement would allow more cost-effective use of intelligence budgets for understanding the design of exported cryptographic systems.

Products providing greater confidentiality should be exportable on an expedited basis to a list of approved companies if the proposed product user is willing to provide access to decrypted information upon legally authorized request. Firms on the list would agree to provide the original version of encrypted information to the U.S. government upon presentation of a proper law enforcement request

The U.S. government should streamline and increase the transparency of the export licensing process for cryptography. Vendors and users alike encounter a great deal of uncertainty regarding rules, time lines, and the criteria used in making decisions about the exportability of particular products. Greater clarity and speed in the export licensing process would go a long way toward reducing the distrust between vendors/users and the U.S. government and would also help to promote the use of cryptography by legitimate users.

The evolution of the information age is likely to create many new challenges for public safety, among them being the greater use of cryptography by criminal elements of society. If law enforcement authorities are unable to gain access to the encrypted communications and stored information of criminals, some criminal prosecutions will be significantly impaired. In order to ensure their access to encrypted information, law enforcement officials support escrowed encryption that would give them authorized access to the decryption key. Driven by law enforcement concerns, the U.S. government has aggressively promoted escrowed encryption since 1993. These promotion efforts have included the promulgation of the Escrowed Encryption Standard for telephone communications, commonly known as the Clipper Chip; a program to develop and deploy hardware products that provide escrowed encryption; and a proposal to condition liberalization of export controls on the implementation of a comprehensive national system.

If escrowed encryption proves feasible and desireable on a large scale, it is a promising technology that may have considerable value to the private sector. But although the government's interest in escrowed encryption is understandable, the present policy of aggressive promotion is unwise for several reasons: the lack of operational experience with a large-scale infrastructure for escrowed encryption and the potential risk to end users that escrowed encryption may be less secure than unescrowed encryption because it is specifically designed to permit access by parties not originally intended to have access to encrypted data; the lack of demonstrated evi-

dence that escrowed encryption will solve the most serious problems that law enforcement authorities face; the likely harmful impact on the natural market development of applications made possible by new information services and technologies; and the uncertainty of the market response to such aggressive promotion.

Escrowed encryption should be a part, but only a part, of an overall strategy for dealing with the problems that encryption poses for law enforcement and national security. An appropriate overall strategy would be based on the following steps:

Relaxation of export controls would help to solidify U.S. leadership in a field critical to national security and economic competitiveness.

The U.S. government should actively encourage the use of cryptography in nonconfidentiality applications such as user authentication and integrity checks. User authentication (verification that the purported sender or author of a message is indeed its real sender or author) and integrity checks (which ensure that data retrieved or received are identical to data originally stored or sent) are particularly important in addressing vulnerabilities of nationally critical information systems and networks. Furthermore, these applications of cryptography are important crime-fighting measures. To date, national cryptography policy has not fully supported such nonconfidentiality uses. For example, the government has acknowledged the need for cryptographically based "digital signatures" but has promoted a standard for digital signatures that is not popular in the marketplace. In addition, government has expressed considerably more concern in the public debate regarding the deleterious impact of widespread cryptography used for confidentiality than over the deleterious impact of not deploying cryptographic capabilities for user authentication and data integrity.

The U.S. government should promote the security of the telecommunications networks more actively. At a minimum, the U.S. government should promote the link encryption of cellular communications and the improvement of security at telephone switches. Link encryption would mean that a cellular call would be encrypted between the mobile handset and ground station, but it would be unencrypted when being carried on the landlines of the telephone network. Such a step would not diminish government access for lawfully authorized wiretaps, because carriers could provide law enforcement with the unencrypted traffic from the landlines. Weak security at telephone switches allows malicious hackers to monitor and reroute telephone calls by dialing into maintenance ports intended to facilitate remote repairs; better access controls could be placed on these ports. By addressing demands for greater security in voice communications that are widely known to be nonsecure, these measures would also reduce the demand for (and thus the availability of) devices used to provide end-to-end encryption of voice communications. Without a ready supply of such devices, a criminal user would have to go to considerable trouble to obtain a device that could thwart a lawfully authorized wiretap.

The U.S. government should explore escrowed encryption for its own uses to better understand how it might operate. To address the critical international dimensions of escrowed communications, the U.S. government should work with other nations on this topic. Many policy benefits can be gained by an operational exploration of escrowed encryption by the U.S. government for government applications. Such exploration would enable the government to develop a base of experience on which to build a more aggressive promotion of escrowed encryption should circumstances develop in such a way that encrypted communications come to pose a significant problem for law enforcement.

Congress should seriously consider legislation that would impose criminal penalties on the use of encrypted communications in interstate commerce with the intent of committing a federal crime. The purpose of such a statute would be to discourage the use of cryptography for illegitimate purposes, thus focusing the weight of the criminal justice system on individuals who are in fact guilty of criminal activity rather than on law-abiding citizens and criminals

alike. Any statute in this area should emphasize deterring the use of encryption for criminal purposes rather than providing yet another possible basis on which to charge a suspected criminal, and should be drafted with safeguards to prevent prosecutorial abuse.

High priority should be given to research, development, and deployment of additional capabilities for use in law enforcement and national security applications in order to cope with new technological challenges. Despite a long history of adaptability to changing technological circumstances, business as usual will not bring agencies responsible for law enforcement and national security into the information age. The nation should give high priority to efforts to develop new technological capabilities that could be deployed during the time that it will take for cryptography to become truly ubiquitous. Such capabilities, including the ability to recover the relevant digital stream from a veritable torrent of data, are almost certain to have a greater impact on future information collection efforts than will attempts to promote escrowed encryption to a resistant market.

Finally, national cryptography policy is only one component of a national information-security policy. Without a forward-looking and comprehensive national information-security policy, changes in national cryptography policy may have little practical effect on U.S. information security. The U.S. government should develop a mechanism to promote information security in the private sector, a mechanism that does not exist today. In the absence of a coordinated approach to promoting information security, the needs of many stakeholders may well be given inadequate attention. Government has an important role to play in actively promoting the security of information systems and networks that are critical to the nation's welfare—for example, the banking and financial system, the public switched telecommunications network, the air traffic control system, and the electric power grid. In other sectors of the economy, the role of the U.S. government should be limited to providing information and expertise.

The national interest will be best served by a policy that fosters a judicious transition toward the broad use of cryptography. Although it is true that the spread of cryptography will sometimes increase the difficulty of the information gathering activities of law enforcement and national security officials, adoption of the recommendations above will lead to enhanced confidentiality and protection of information for individuals and companies, thereby reducing economic and financial crimes and economic espionage from both domestic and foreign sources. In addition, they will result in a more secure national information infrastructure. Thus, these recommendations will contribute to the prevention of crime and enhancement of national security. On balance, the advantages of widespread commercial and private use of cryptography clearly outweigh its disadvantages.