

Q: Should Uncle Sam control U.S. encryption technology exports?

Yes: Export controls will help maintain U.S. market share of future encryption products.

BY WILLIAM A. REINSCH



Reinsch is the undersecretary of commerce for export administration and an adjunct associate professor at the University of Maryland at College Park.

Making strong commercial encryption widely available indeed is in our country's best interests. It is inevitable that powerful computers, advanced telecommunications and broad electronic networks will form the basis for communications and commerce in the future. Encryption will be essential for the full development of electronic commerce in networks. Businesses and individuals need the means to protect sensitive commercial information from fraud and industrial espionage and to preserve privacy, and their demand for these products will further the spread of encryption. We must shape our export-control policies so that, in their pursuit of global markets, U.S. companies can take full advantage of their strengths in information technology.

But the increased use of encryption carries with it serious risks for public safety and our national security. Any policy on encryption must address these risks as well if it is to be in the national interest. Our policy provides that balance by working in close consultation with the private sector and by working with the market, not against it.

A successful national policy must answer two important questions: How do we ensure that communications across public networks are trustworthy and conducted with security and integrity? How do we accommodate the communications requirements of individuals and businesses while still fulfilling our obligations to protect American public safety and U.S. national security?

First, we need electronic services that would build trust in encryption systems. These are called key-management, or security-management, infrastructures. They would provide

the services of a "certificate authority" that would verify encryption keys through the use of a digital signature, a technique that also can verify both the originator of a message and the integrity of that communication. Just as an individual's personal signature or a notary public's stamp provides credibility and verification to paper documents and transactions, digital signatures will do the same for electronic communications.

With the advent of public-key cryptography and the inclusion of encryption capabilities in mass-marketed software, encryption now is available to more users than ever before. However, for encryption to be used on a broad scale in electronic commerce — home banking and legal transactions, for example — users must have the same level of confidence they have in paper transactions.

The ability of encryption users to access backup-encryption keys can be critically important to individuals, businesses and law enforcement. Just as homeowners leave keys to their houses with neighbors or friends in case they accidentally are locked out, encryption users must be able to access extra keys if theirs are lost. This particularly is true of users who plan to encrypt crucial financial or corporate information in today's unbreakable encryption. For example, the 56-bit digital encryption standard, or DES, recently was advertised as breakable after 78,000 workstation computers working for 96 days solved one message. If I encrypted my will using DES, my heirs would face the same hurdle to access it — an irksome task. However, if they were able to access my keys from a key-recovery agent, my will would be available quickly once they had established a legal authority to access the information.

In the same way, without some means of accessing encrypted information, law enforcement, when it exercises court-ordered wiretaps and searches in criminal cases, will have lost an important tool in prosecuting felonies such as drug-trafficking, kidnappings and terrorism. However implemented, key recovery should be initiated and operated by the private sector. The Clinton adminis-

(continued on page 26)

No: These controls threaten the privacy of law-abiding citizens and send U.S. jobs overseas.

BY BOB GOODLATTE



Goodlatte, a Virginia Republican, serves on the House Agriculture and Judiciary committees and is the sponsor of the Security And Freedom through Encryption Act of 1997.

Strong encryption products are the locks and keys of the digital age. Simply defined, encryption is the use of data-scrambling software to secure communications and computer information so intruders cannot access them. In the industrial age, encryption chiefly was used only by spies and the military; in the information age, however, the whole world is beginning to realize the importance of protecting digital communications and on-line transactions. Just as deadbolt locks and alarm systems help people protect their houses against intruders, thereby assisting law enforcement in preventing crime, strong encryption allows people to protect their digital communications and computer systems against criminal hackers and computer thieves.

At present the digital world is not a safe place to do business. Criminal hackers and computer thieves readily can intercept sensitive personal and proprietary business information. Economic espionage costs American businesses tens of billions of dollars every year. Stories about the theft of credit-card numbers on the Internet are being reported with increasing frequency. And even the FBI, in its 1998 budget request, has called this situation "a rapidly escalating crime problem," estimating that the Pentagon's computers are subject to hackers' attempts to break into them 250,000 times a year.

America's computer industry has responded to the increasing demand for on-line security by developing state-of-the-art encryption products. However, the Clinton administration, while professing support for the widespread use of strong encryption, continues to enforce antiquated policies that prevent U.S. companies from exporting strong, market-driven encryption products — even though they are widely available from foreign manufacturers and on the Internet. Clearly, the administration's encryption policies are at odds with its stated goals.

To address this growing problem, Rep. Zoe Lofgren, a California Democrat, and I have introduced HR695 — the Security and Freedom through Encryption, or SAFE, Act of 1997. This bill accomplishes three critical goals: preventing economic crime, promoting electronic commerce and protecting the personal privacy of all law-abiding Americans.

HR695 enjoys the support of organizations across the political spectrum. A partial list of supporters includes the U.S. Chamber of Commerce, the National Association of Manufacturers, the Law Enforcement Alliance of America, the Business Software Alliance, the Computer and Commu-

nications Industry Association, the Information Technology Association of America, Netscape, Microsoft, Americans for Tax Reform, the Eagle Forum, the National Rifle Association, the American Civil Liberties Union and the Center for Democracy and Technology. These organizations understand the importance of encryption to commerce and privacy in the information age, and believe the SAFE Act is the right approach to providing computer users with the safety and security they need.

As noted, HR695 prevents economic espionage while protecting hundreds of thousands of American jobs. This legislation has four main components: (1) Ensuring all Americans the freedom to use and sell any type of encryption domestically; (2) prohibiting the government from mandating that people use "key-recovery" or "key-escrow" encryption, in which computer users are required to give the government access to their communications and computer files without their knowledge; (3) creating a level playing field for American business in the global marketplace by allowing the export of generally available encryption products; and (4) creating additional criminal penalties for those who knowingly use encryption to coverup federal felonies.

While allowing the export of generally available encryption, the SAFE Act does not allow the export of sensitive military or weapons technologies. The integrity of our national-security infrastructure is dependent upon keeping such technologies secret, and HR695 will not change our current policies in that area. What the bill does allow to be exported, however, are products that can be purchased at a local computer store or over the Internet.

The Clinton administration, unfortunately, prefers to pursue a policy that not only keeps American companies from fully competing with foreign manufacturers but also seeks to impose bureaucratic regulatory schemes on the marketplace. The administration is attempting to create these regulatory schemes under the umbrella of broad new "key-management infrastructures" that have yet to be tested in the marketplace.

Driven by user needs, the on-line world is developing such systems of assurance without government intervention. The security and effectiveness of these systems will be tested by the market. Consequently, it is impossible to know at this point which systems will succeed and which will fail — the intensely competitive global marketplace will decide that question. Government bureaucracy and regulation neither is necessary nor desirable.

By preventing American companies from exporting strong encryption, the government perpetuated a sense of uncertainty in the marketplace that has discouraged these companies from developing commercial infrastructures. On the other hand, HR695 actually promotes the development of such infrastructures by removing unwanted and unworkable government regulation. As former British *(continued on page 27)*

REINSCH: continued from page 24

tration consistently has stated that the government does not wish to hold the keys to encrypted communications.

All of these security-management services are crucial to the development of electronic commerce and the conduct of everyday business on the Internet. Voluntary registration of certificate authorities and key-recovery agents will lend credibility to these services and ensure the client that minimal responsibility standards have been met. In turn, protection from civil and criminal liability should be afforded these providers.

Controls of strong encryption exports play an important role in the implementation of this secure public-network policy and in the preservation of national security and law enforcement. They permit the government to review license applications, the proposed end user and other information which may harm U.S. law-enforcement or national-security interests. The Clinton administration believes those risks to national security from international crime, terrorism and drug-trafficking also justify continued controls and government review.

In that regard, export controls are consistent with America's international obligations under the Wassenaar Arrangement to Voluntary Restraint Agreements. A number of U.S. trading partners have gone beyond our controls and imposed more-rigorous import restrictions or domestic-use requirements. Through our special envoy for encryption, Ambassador David Aaron, the United States is pursuing discussions with other governments to reach common approaches toward key-management infrastructures the world over. These infrastructures will facilitate electronic communication and commerce internationally and expand the market for American products while maintaining appropriate access for the purposes of law enforcement.

That latter point is particularly important because it goes to the heart of Virginia Republican Rep. Bob Goodlatte's arguments. To his credit, he has recognized the need for secure infrastructures. At a May 1997 hearing on his bill, he said, "We have to promote the use of key management and key recovery because, if anybody sets up a heavily encrypted computer system and loses their key or hasn't the ability to communicate with some aspect of their communications system, they have created an enormous problem for themselves, risking huge economic loss by doing so." Despite this acknowledgment of the value of key-management infrastructures, he continues to pursue legislation which does absolutely nothing to promote their development.

Instead, Goodlatte has chosen to focus on a single piece of the encryption-policy puzzle: how to ensure that U.S. manufacturers of encryption products can compete effectively in the international marketplace. But his solution — elimination of export controls on all encryption hardware and software — misses a fundamental point about the market. Encryption

products are going to be most in demand when the infrastructures within which they can function are in existence. Without key-management infrastructures, without digital signatures, using strong encryption is like putting a combination lock on a cardboard box — it looks fine, but the security is an illusion.

In other words, simply allowing U.S. producers unrestricted sales abroad will not make them competitive. Instead, we need to promote key-management infrastructures, authentication systems such as digital signatures and greater interoperability so that different systems can talk to each other. Goodlatte's approach will not do that. On the other hand, S909, the Secure Public Networks Act, introduced by Democratic Sen. Robert Kerrey of Nebraska and Republican Sen. John McCain

of Arizona, will. If the United States establishes these basic elements of secure public networks internationally, American producers doubtless will maintain or increase their current overwhelming share of the market. That is why the Clinton administration is spending so much time in discussions with our trading partners to develop a common approach. Even if we do not forge a shared approach to key management, however, it is highly unlikely that the result would be free trade in encryption products. Simply removing

export controls at our end by no means is a guarantee that other nations will let our products in.

No one is more eager to promote American products than the Commerce Department, where I serve, but immediate decontrol of exports will not have that result. It could, however, degrade the nation's ability to produce vital intelligence for military commanders and undermine U.S. efforts to protect Americans from terrorists, spies and drug traffickers. With the Clinton administration's policy we can avoid paying that price at the same time we develop the infrastructures that in fact will demand appropriate U.S. products.

The best proof of our policy is American industry's response to it. We have provided more-liberal export controls for those companies that commit to build key-recovery products in the future. In the first seven months we have received more than 1,000 license applications for exports valued above \$500 million. Thirty-three companies have submitted commitment plans which lay out how they will build and market key-recovery products, and we have approved 29. These companies include some of the largest software and hardware manufacturers in the country.

This is a difficult public-policy issue and it demands more serious attention than it has received thus far. We must focus our attention on fitting together the various pieces of the encryption-policy puzzle to form an approach that balances all the public interests without jeopardizing national security or public safety.

Many Americans are aware of the complexity of this issue, particularly members of Congress, private-industry leaders, members of the Clinton administration and computer buffs. Because of the complexity of the issues, the information avail-

Decontrol of exports could degrade the nation's ability to produce vital intelligence for military commanders.

able to the average American does not convey the impact this policy will have on how business and private communications are conducted across the Internet. Many Americans do not understand that the resolution of this policy debate ultimately will decide whether they will be able to trust the Internet for electronic commerce. We owe our citizens a comprehensive

resolution of all the issues affecting them and a policy that balances the use of strong encryption with the need to preserve national security and allow law enforcement to continue its commitment to protecting public safety. We cannot be satisfied with one-sided proposals that do not even attempt to meet all of the public interests involved. •

GOODLATTE: continued from page 25

Prime Minister Margaret Thatcher aptly put it, "Governments ... are themselves 'blind forces' blundering about in the dark, and obstructing the operations of markets rather than improving them."

A recent report issued by 11 of the world's top cryptographers, titled *The Risks of Key Recovery, Key Escrow and Trusted Third Party Encryption*, offers further evidence that various key-escrow, key-recovery and key-management systems proposed by the administration neither are feasible nor advisable. This report found not only that "the field of cryptography has no experience in deploying secure systems of this scope and complexity," but also that such systems involve security risks and potentially could cost many billions of dollars.

In addition to the feasibility questions surrounding the administration's attempt to link digital signatures, certificate authorities and key-recovery encryption into a global key-management infrastructure, this approach raises serious constitutional questions as well. First Amendment guarantees of freedom of speech, Fourth Amendment protections against unreasonable searches and seizures, Fifth Amendment rights against self-incrimination and 10th Amendment reservations of powers to the states all are implicated in the administration's proposal. Surrendering constitutional rights is too high a price to pay for participating in electronic commerce.

The administration continues to claim that strong encryption is not widely available overseas, in part because of U.S. export controls. However, this assertion ignores the fact that German, Dutch, Swedish, British, Russian and other foreign manufacturers have created more than 500 strong and reliable encryption products that are available internationally and on the Internet. As one article noted, "Far from hindering the spread of powerful encryption programs, American policy has created a bonanza for alert entrepreneurs outside the United States."

An example of the folly of the administration's export restrictions is the recent announcement that Sun Microsystems will be entering into a partnership with Elvis+, a Russian encryption manufacturer, to distribute strong encryption worldwide. Since the United States has no import or domestic controls on the use of non-key-escrow encryption (and rightly so), Sun can import the Russian product and distribute it domestically, while the Russian company distributes the same prod-

uct overseas. Therefore, U.S. companies now will be able to communicate securely with their overseas offices and subsidiaries without violating the export-control laws; unfortunately, they will not be using U.S.-made encryption products to do so. Even worse, we will be exporting thousands of jobs overseas to create and sell encryption products that should be made in America.

The Sun announcement demonstrates three critical facts that reveal the absurdity of arguments the administration uses to defend its current policies: (1) Consumers are demanding strong encryption products to protect their digital communications; (2) strong encryption products already are available from foreign manufacturers, and reputable U.S. firms are willing to stake their corporate reputations on the quality of those products; and (3) the current export-control scheme is taking jobs and revenue from our economy.

In addition to promoting electronic commerce and protecting personal privacy, strong encryption prevents crime. In its landmark report on encryption policy, the blue-ribbon National Research Council concluded the following: "If cryptography can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States."

The administration's encryption policy actually undermines our national security by keeping strong, market-driven, American-made encryption products from dominating the global marketplace. Proliferation of American encryption products is essential if we are to preserve the integrity of our national-security infrastructure in the information age. If U.S. encryption continues to be restricted, however, foreign products soon will dominate the marketplace, hindering our ability to gather effectively intelligence against terrorists and criminals.

The SAFE Act prevents economic crime, promotes electronic commerce and protects the personal privacy of all law-abiding Americans. Additionally, it allows the free market to design its own standards and solutions for the development of global commerce, free from unwanted and unworkable government regulation. This bipartisan legislation ensures that all law-abiding Americans will be able to communicate privately and conduct business securely in the information age. •

Surrendering First, Fourth, Fifth and 10th Amendment rights is too high a price to pay for electronic commerce.