

Domestic Encryption Controls

U.S. citizens today enjoy the right to develop, distribute, and use very strong encryption within the United States.¹⁰² The administration has stated that "no restrictions apply to the U.S. domestic use of cryptography, and the Administration has no plan to seek restrictions."¹⁰³

But some lawmakers, and FBI director Louis Freeh have proposed requiring key recovery within the United States, that is, outlawing the domestic use of encryption that does not support key recovery.¹⁰⁴ Freeh argued that encryption

used in the United States or imported into the United States for use [should] include a feature which would allow for the immediate, lawful decryption of the communications or the electronic information.¹⁰⁵

Thus pressure to outlaw nonescrow encryption within the United States is likely to continue.

University of Chicago law professor Richard Epstein has testified that the Fourth Amendment would forbid mandatory domestic key escrow, as the amendment is triggered by any request for secret keys.¹⁰⁶ Perhaps, then, mandatory key recovery is out of the question for domestic markets, particularly as it is articulately opposed by Senate Majority Leader Trent Lott.¹⁰⁷

That leaves the government with the option of pursuing "voluntary" key recovery. But the key-recovery schemes the current administration supports would be "voluntary" in name only, as discussed below in the section on the future of encryption legislation.¹⁰⁸

"Balance" and Compromise

Administration officials often respond to critics of encryption export controls by calling for "balance." John Hamre, Deputy Secretary of Defense, states that "the government is searching for an approach that balances the needs of individual privacy, public safety, business and national security. All are important."¹⁰⁹ Certainly, one would not want to appear to advocate an unbalanced approach. The encryption debate is about where the balance should be struck. The framers of the U.S. Constitution decided that, on balance, the power of the federal government to regulate communications (free speech and

the press) should be very limited. Likewise, the Fourth Amendment manifests the view that the police have a right to search through our papers to look for incriminating messages after they have obtained a warrant--but not a power to forbid us to encrypt our messages. The view that encryption technology should be freed from export controls and key-recovery mandates maintains that constitutional balance.

Regulators urge software and hardware firms to cater to demands for "balance" by offering features to aid law enforcement.¹¹⁰ Sometimes, however, no new features are necessary to provide authorities with the access they request. One example is the "private doorbell" or ClearZone proposal, proffered by Cisco Systems and joined by 12 of the nation's largest technology firms asking for clearance to export similar products.¹¹¹ ClearZone provides network encryption only, that is, the product does not encrypt information moving through your modem or through your Local Area Network. Once it reaches your Internet Service Provider's router, it is encrypted using triple-DES before being sent on its way across the Internet. Should an FBI agent want to see the plaintext of the message, he hands your ISP's system administrator a warrant. The administrator flips a "network control switch" that lets the agent see everything you do through a temporary "dynamic access point" before it is encrypted by the routers.¹¹² Of course, you could still use PGP to encrypt the message before it reaches the routers, but this would not be Cisco's responsibility.

Clearly, however, ClearZone cannot and was not intended to mark the end of the struggle to free encryption technology for export. Export of network encryption

- offers no relief for the sale of point-to-point encryption products like PGP, which encrypt messages on the user's computer, and
- offers no relief for the sale of real-time encryption products, which encrypt your files as you work on them.¹¹³

And the use of network encryption alone requires the user to trust a third party, the ISP, to secure his privacy. However, there is no reason that routers enabled to provide encryption should not be freely exported.

The Effect and Efficacy of Export Controls

Export controls have hurt software developers within the United States, who are barred from selling strong encryption technology in markets worldwide. While recent reforms do open some markets to U.S. encryption developers, the impact will continue in those market segments that have not been freed. Supporters of continued controls urge that this cost is balanced by benefits to law enforcement. This section shows that wherever they remain, export controls hurt national security more than they help.

Unilateral or Universal Controls?

In 1982, a major study of national security interests in controlling information about technology noted that export controls helped more than they hurt only when the United States is the only source of information about the technology, or other friendly nations that could also be the source have control systems as secure as ours."¹¹⁴ Many American officials acknowledge the essential truth of this.¹¹⁵

This necessary condition for the success of export controls does not hold for encryption. A bare handful of countries, mostly undemocratic ones such as Belarus, China, Pakistan, and Russia, impose domestic controls on the use of encryption. France and the United Kingdom can expect pressure to lift their policy of supporting key access to conform with the policy of the European Union.¹¹⁶ While members of the European Union do license the export of cryptography, they have strongly resisted enforcing those controls as strictly as the United States¹¹⁷--opposing, for example, the requirement that exported products support key escrow.¹¹⁸ Many countries do not and are not expected to have export controls. The vast majority of countries offer safe havens for the manufacture, use, and distribution of encryption and are expected to continue to do so.¹¹⁹

The Clinton administration has lobbied hard before the Organization for Economic Cooperation and Development, sending police rather than economists as U.S. representatives to ensure that there will be no safe havens. The administration has appointed a roving "crypto czar," David Aaron, to visit foreign governments and argue in favor of universal controls on encryption.

These ventures have met with limited success only in the United Kingdom,¹²⁰ Canada, and Japan.¹²¹ The OECD

rejected the United States' plans to establish universal mandatory key escrow, as has the Australian Walsh Report.¹²² The European Commission's Directorate-General, responsible for developing information policy for the European Union, recognizes that

restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks. It would not however prevent totally criminals from using these technologies.¹²³

The commission therefore believes that regulation and provisions for law enforcement access should be minimal. Detlef Eckert, chief adviser on encryption policy at the European Commission, has said that "encryption technologies should be allowed to emerge in the marketplace. They should not be regulated, as the United States government has suggested."¹²⁴ Oddly, Vice President Gore reportedly is unaware of these developments, perceiving the administration's position to be a widely acceptable compromise.¹²⁵

Given these trends, universal controls will never be adopted. Certainly, no widespread regulatory regime will be adopted within the next five to ten years--ample time for software developers working in the United States to lose their competitive edge--in any encryption market they have not been permitted to tap. The following sections therefore describe the impact of export controls, assuming that many or most countries will not adopt similar controls.

The Burden of Export Controls to Individual Companies

Export controls impose substantial costs on developers of software or hardware attempting to sell their products in foreign markets, including the the cost in money and time of submitting to review. Even within the United States, companies may require a license to release encryption products to their own employees who happen to be foreign nationals.¹²⁶ Products still face review not only by the Bureau of Export Administration but also by the Department of Justice, the National Security Agency, and the FBI;¹²⁷ the FBI is reportedly causing delays from one to six weeks in licensing reviews.¹²⁸

Product designers are always uncertain which algorithms will be approved. In the future, encryption programs might be so entirely integrated within applications that almost every item of software and hardware would

become an "encryption product" subjected to review. In the future, automatic programming systems might use very general instructions to create encryption programs, though it would difficult to distinguish these instructions from ordinary speech.¹²⁹

The Commerce department must review not only whether an encryption product supports key recovery or only offers "weak" crypto, but also ensure key-recovery features cannot be disabled or bit length expanded. Netscape, for example, sells "crippled" versions of its browsers to overseas customers (56-bit instead of 128-bit). But removing the limits is pitifully simple. Open the browser with a text editor such as BBEdit or Emacs. Search for "SSL2-RC4-128-EXPORT40-WITH-MD5," to find a table that looks like this:

Export policy

Software-Version:	Mozilla/4.0P3
PKCS12-DES-EDE3:	false
PKCS12-DES-56:	false
PKCS12-RC2-40:	true
SSL2-RC4-128-WITH-MD5:	false
SSL2-RC2-128-CBC-WITH-MD5:	false
SSL2-DES-168-EDE3-CBC-WITH-MD5:	false
SSL2-RC4-128-EXPORT40-CBC-WITH-MD5:	true
SSL3-FORTEZZA-DMS-WITH-RC4-128-SHA:	false
SSL3-RSA-WITH-RC4-128-MD5:	conditional
SSL3-RSA-WITH-RC2-CBC-40-MD5:	true

To enable strong encryption, simply change all the "false" and "conditional" lines to "true." An Australian product called Fortify does just that.¹³⁰ Commerce reviewers will catch few of these features, but will add endless delays and expense while they try.

Export controls also add to product distribution costs. The controls prevented Netscape from using the Internet to distribute the "strong crypto" version of its browser to foreign citizens.¹³¹ Companies want the freedom

to distribute beta versions of their product over the Net, so that bugs can be fixed before commercial distribution.

In fast-moving technology markets, these costs, which need not be incurred by foreign competitors, will prove fatal to the success of many new product ventures.

Export Control's Impact on Domestic Security

Export controls make the use of strong encryption technology in domestic markets less likely.¹³² This will prove costly by making domestic communications less secure. Because the recent sectoral reforms primarily benefit a few large-scale corporate users, mass-market products for the use of individuals will continue to stagnate. Export controls force domestic encryption producers to design one product for the unrestricted domestic market and another for export--or forgo serving one of the two markets. The cost of research and development can preclude developing two versions of a product. Because about half of sales of U.S. information technology products are to foreign customers,¹³³ vendors often choose to serve only the foreign market, which results in a product of limited bit length.

Export controls make it more likely that weak encryption will be widely used domestically even if a strong version is available. Because of export controls, the strong version of Netscape, which offers 128 bit crypto, cannot be sold over the Internet. It is only sold in shrinkwrapped packages in stores. Because the weaker, exportable version is available free over the Internet, this version is more widely used even within the United States.¹³⁴

Finally, export controls delay the widespread deployment of encryption in both domestic and international markets by creating a climate of uncertainty.¹³⁵ The National Research Council found that worldwide removal of all controls on the export and import of encryption products would result in more rapid standardization of those products, and more widespread use.¹³⁶

The widespread use of strong encryption would bring gains in network security that should not be overlooked in the debate about national security.¹³⁷ Law enforcement interests naturally think of themselves as the nation's first line of defense against espionage and terrorism, but today's computer networks are highly decentralized. Since the hardware and software are in the hands of myriad users subject to attack from many different network access

points, security should be decentralized as well. The FBI and the NSA do little to guard the private sector against computer viruses; the private sector uses software to protect itself. Widespread use of strong encryption will be the nation's first line of defense against terrorists and criminals, just as a lock on the door is the first line of defense against theft. Federal law enforcement will provide essential backup.

Because of these effects, the greater mass of harmless communications within the United States will be vulnerable. At the same time, strong encryption without key-recovery features will continue to be available to criminals and terrorists.

The Futility of Export Controls

Export controls can be used to stop hard-to-transport items like missiles or military planes from leaving the country. But they cannot stop the spread of a few lines of code (an encryption program can be contained in as few as three lines), technology that can be transported instantaneously over phone lines at almost no cost. Nor can they stop the movement of capital abroad to software developers located in other countries.

The Inexorable Growth of Foreign Competitors. The costs of export controls give companies located in less restrictive foreign countries a strong advantage.¹³⁸ Thawte Consulting, Inc. of South Africa makes Internet software offering 128 bit encryption and distributes it over the Internet, advertising that its technology is not restricted by export controls.¹³⁹

A wide range of encryption products made by at least 440 foreign companies are already available in international markets, some distributed over the Internet.¹⁴⁰ As of this writing, almost 656 such products are commercially manufactured, and many of these products offer stronger encryption than can legally be exported from the United States.¹⁴¹ While it has been claimed (but not proven) that some of these products are of inferior quality,¹⁴² there is no inherent reason that they should be or would long remain so.

The evolving business model uses the Internet to supply strong encryption using Secure Socket Layer (SSL) proxy servers. Customers may be leery of products distributed over the Internet from an unknown source, but the list of reputable "brand name" products is growing.

Encryption using products like SSLeay, SSL source code available free from a web site in Australia, enables the creation of strong encryption products from weaker products. Stronghold, a UK product, combines SSLeay with Apache, a leading Web server in the public domain, to create a 128 bit Web server. Other products that use the SSL include Zeus, SafePassage (both from the UK), Oyster (Australia), Brokat (Germany), R3 (Switzerland), Baltimore (Ireland), Data Fellow (Finland), and FICS (Belgium). These vendors fill a gap in the market left by Internet browsers crippled by U.S. export controls. The market for messaging systems is moving in the same direction, as security protocols (S/MIME) are published using widely available source code and algorithms.

The impact of the 40-bit limit is illustrated by a case involving Netscape. A large corporation in Germany considered using Netscape's 128 bit key software to establish a sophisticated national health-care data network based on "smart cards." Netscape, however, could not provide the software because of export controls. So the German government had a German company build the software from scratch. "This not only means a loss of a sale to Netscape. It also means that a new competitor has been created where one did not exist before."¹⁴ The new sectoral reforms mean that this problem may not occur again with health care, but instead with biochemical or pharmaceutical manufacturing.

Domestic companies generally cooperate with law enforcement authorities when they face difficulties with decoding encrypted messages. The next generation of advanced encryption technology for e-mail or real-time communications is unlikely to be developed within the United States. U.S. law enforcement authorities are unlikely to find cryptographers based in India, Israel, or South Africa helpful in solving difficult encryption problems.

The Movement of Talent, Jobs, and Capital Abroad. As long as export controls are maintained, jobs, capital, and profits will leave the United States as technology companies set up operations elsewhere.

Under ITAR, the transfer of technology abroad could be accomplished by licensing; the owner of a U.S. encryption invention could license the right to have it built in a foreign safe haven--and then import it into the United States. RSA, for example, created subsidiaries in the People's Republic of China and in Japan to do joint research on encryption software. The Japanese subsidiary reverse engineered RSA's U.S. product, so RSA did not vio-

late any export rules.¹⁴⁴ Export controls likewise have not stopped a foreign company from buying control of a U.S. company that produces encryption technology.¹⁴⁵

The new regulations attempt to control this type of activity by rigorously controlling "reexport" of U.S. technology--a move guaranteed to make capital that would have gone to U.S. companies flow abroad. Sun Microsystems thus bought 10 percent of a Russian supplier to sell encryption software to overseas customers.¹⁴⁶

Developers who use this tactic will face pressure from the government--such as the threat of the loss of government contracts--to abandon their oversea efforts. That simply means, however, that the next generation of encryption products developed abroad will not involve any technology developed in the United States. U.S. companies and investors will move all their development and capital abroad. While Microsoft is unlikely to abandon its extensive operations in Washington state for parts unknown, the next Microsoft or Netscape will simply never start up domestic operations.

How Code Moves across Borders. Strong encryption developed in this country can easily be smuggled abroad.¹⁴⁷ All it takes is a public telephone line and a computer modem, a disk tucked into a suitcase (legal, under the personal use exemption),¹⁴⁸ or someone posting the product anonymously on the Internet, as was PGP.

The recent (legal) export of PGP speaks eloquently to the futility of controls. A book containing the source code for PGP was mailed to Norway by a venturesome cypher-punk.¹⁴⁹ Norwegian volunteers scanned the pages containing the code into computers and soon after the book's arrival had compiled a working copy of PGP software, which these Vikings of the cyberseas promptly posted on the Internet.¹⁵⁰

One supporter of continued controls argues that smugglers can move good over the border by driving out into the desert and crossing in the middle of the wilderness, but most choose instead to stick to the road and risk going through the check point, assuming that the smuggled goods would not be found in a search. That analogy does not work for applied to encryption. Unlike driving out into the middle of the desert, obtaining and using bootleg encryption will cost the criminal no more effort than a click of the mouse button on the Internet.

Even in a world where most or all countries outlawed nonescrow encryption, any programmer could create an effective encryption program using information published in academic journals that publish articles on the algorithms used in cryptography.¹⁵¹ Books such as the readily available classic Applied Cryptography reprint the source code for existing encryption programs; a competent programmer could create his own program by typing this source code into a computer. In a statement seconded by many other authorities, Nathan Myhrvold of Microsoft testified that

any competent programmer, including thousands of young "hackers," could easily write software or use off-the-shelf, low-cost personal computers to impose encryption on digital data, including digital voice transmission. The fact that it is so easy to defeat the system means that organized crime or anyone seriously intent on escaping the FBI's scrutiny would be able to do so.¹⁵²

Criminals could hide their use of nonescrow encryption by using multiple encryption. The outer encryption layer would use key escrow, to avert suspicion. The inner layer would not.

The National Research Council lists several other evasion techniques, including

- the use of data formats other than ASCII;
- the use of an obscure plaintext language, such as Navajo; and
- the use of steganography, the art of hiding one message within another message or a picture (such as a black and white photograph).¹⁵³

What's Left for Law Enforcement?

To summarize, the benefits of export controls to law enforcement are greatly eroded by

- weaker domestic and international security because of the effect of export controls on the availability and cost of strong encryption,
- the takeover of encryption innovation by foreign competitors unlikely to cooperate with police in the United States, and

- the ease of evading export controls and key-recovery mechanisms.

Supporters of export controls have responded weakly to these objections. They explain that they do not want access to all message traffic. Rather, they hope to intercept criminal's communications with innocent parties:

It is worth noting that we have never contended that a key escrow regime, whether voluntarily or mandatorily implemented, would prevent all criminals from obtaining non-key escrowed encryption products. But even criminals need to communicate with others nationally and internationally, including not just their criminal confederates but also legitimate organization such as banks.¹⁵⁴

Terrorists are unlikely, however, to provide their bankers with details of their nefarious plans. And law enforcement would usually be able to depend on the cooperation of the innocent party, or on subpoena of their records.

Compared to security losses due to export controls, the gains to law enforcement seem speculative at best, hardly a sound basis for eroding citizens' privacy and forcing sectors of the United States software industry abroad.

A Closer Look at Key Recovery

Restrictions on the export of encryption software are but one aspect of the regulatory regime for encryption technology. The other side of the coin is that the export of encryption that does incorporate approved "key-recovery" features will be permitted to 42 countries after one-time review. The following section explores the costs and benefits of such government-prescribed key recovery.

The Limited Private-Sector Need for Key Recovery

The administration argues that end users need a "key management infrastructure" in case they need access to an extra copy of their own keys. "Keys can be lost, stolen, or forgotten--rendering encrypted data useless."¹⁵⁵ Conveniently, the end user's "desire for data recovery and law enforcement's potential need for access can be accommodated in a single locale, so long as the user trusts the key storage and law enforcement has confidentiality of access."¹⁵⁶

Private-sector computer users might choose to keep a copy of their keys to retrieve stored data in encrypted form. But they have no need to save the copies of keys used to encrypt real-time communications or many one-time communications:

There is little if any commercial demand for a key-recovery function in real-time communications. The reason is simple: if the communication is unsuccessful then it is simply tried again until the transfer of information is successfully completed.¹⁵⁷

If a business sends a document that is to be decrypted at its final destination, there is no need to keep the key.

By contrast, law enforcement interests demand key-recovery systems that will give them access to all encrypted communications in real time. Louis Freeh, director of the FBI, admits that business does not need real-time key recovery when he says, "law enforcement has a unique public safety requirement in the area of perishable communications which are in transit (telephone calls, e-mails, etc.). It is law enforcement, not corporations, that has a need for timely decryption of communications in transit."¹⁵⁸

The private-sector user of key recovery for stored communications will hardly be anxious to turn his key over to a third party. The third party would have to observe elaborate procedures to ensure that the entity was really entitled to recover the key. The storage of vast quantities of secret key information by any private or government "key-recovery" centers would create a substantial security risk. The centers would become targets for hackers, spies, and infiltrating foreign agents.¹⁵⁹ This security risk raises a tangle of liability issues--the key-recovery agent must either be insulated from liability if the keys are exposed, or else would have no incentive to inform the customer of the breach of security.

Clearly, the simplest way for a user to have easy access to an extra copy of his key is to store an extra copy somewhere on his own premises, in a safe deposit box, with another agent of his employer, or, perhaps, when he chooses, with a third party. This logical option, known as "self-escrow," is exactly what law enforcement does not want, for "in those cases in which an individual or corporation serves as its own certificate authority, government organizations could be compelled to request escrowed key

from the subject of an investigation. The investigation could be compromised under such circumstances."¹⁶⁰

In short, key-recovery mechanisms that ensure law enforcement access to the plain text of communications in real time would be counterproductive for the private sector.¹⁶¹

The Implausibility of Proposals for Key-Recovery Infrastructure

Evidence is mounting that a widely usable key access infrastructure that would allow law enforcement officers to have access to encrypted communications cannot be created. A recent report by a group of cryptographers and computer scientists concludes that key recovery will be too expensive and cumbersome for many uses and users:

All key-recovery systems require the existence of a highly sensitive and highly-available secret key or collection of keys that must be maintained in a secure manner over an extended time period. The systems must make decryption information quickly accessible to law enforcement agencies without notice to the key owners. These basic requirements make the problem of general key recovery difficult and expensive--and potentially too insecure and too costly for many applications and many users.¹⁶²

The National Institute of Standards and Technology committee in charge of designing a federal standard for key recovery failed to complete their task because they encountered "significant technical problems."¹⁶³ The private sector has not yet developed the infrastructure the partial relaxation of export controls was intended to spur.¹⁶⁴

The first obstacle is developing a mass-market product that supports key recovery, particularly for real-time communications. The Business Software Alliance notes that this might not be possible at all:

Some in government seem intent on arguing that because a few products can technically perform key recovery for communications it should be a widespread requirement. To the contrary, our members have seen nothing to suggest that any product developed to date can work on a mass

market scale or that there is significant commercial demand for such products.¹⁶⁵

One difficulty would be the sheer volume of keys that the networks will generate. James Barksdale of Netscape has testified that

in a few short years, there will be nearly 200 million people connected to each other over the Internet. Each of these people is likely to use dozens, if not hundreds, of separate keys in the course of a month of transmission. The sheer volume, speed and breadth of Internet communications daily may soon outstrip most any amount of manpower available to decrypt (with the escrow key) a single communication between suspects.¹⁶⁶

Associated with this first problem is a second, which is surmounting the difficulties of providing key-recovery mechanisms will be prohibitively expensive, particularly for real-time communications. George Spix of Microsoft estimates that the charge for developing any kind of key management infrastructure would run in excess of \$5 billion per year (assuming 100 million users at an assumed cost of \$50 per year, an optimistic 1/10th the per-key cost of the current escrow system used by the government for its Fortezza security product); some estimates run as high as \$100 billion a year.¹⁶⁷ Though some estimates are as low as \$5-10 million, this seems unlikely in light of the technical problems involved.

Legislative efforts to use indirect economic pressures to urge the market towards government-approved key-recovery mechanisms are unlikely to work for the majority of users; non-key-recovery technology will be substantially cheaper. In the absence of key-recovery mandates, electronic businesses catering to the mass market will simply provide security features without charge to the customer, just as businesses today do not charge for locking their doors.

Another problem linked to the technical difficulties of giving law enforcement access, particularly to real-time communications, is the delay factor. Electronic commerce is ready to proceed now. But no mass-market key-recovery infrastructure is now in place, and none can be expected for several years. By the time the technical difficulties have been surmounted and third-party key-recovery agents developed, non-key-recovery technology will have proliferated worldwide--as indeed PGP already has. Underscoring the expense and technical difficulties of developing a working key escrow system is the reluctance of police

forces to use "escrowed" encryption products such as radios in patrol cars:

[The escrowed products] are more costly and less efficient than non-escrowed products. There can be long gaps in reception due to the escrow features--sometimes as long as a ten second pause. Our own police do not use recoverable encryption products; they buy the same non-escrowable products used by their counterparts in Europe and Japan.¹⁶⁸

This same memo notes that some government agencies are expected to reject key recovery because of fears of espionage by foreign governments. And the NSA itself has recently released a report outlining the security dangers of key-recovery products.¹⁶⁹

The Dangers of Government Abuse

In 1930, the Weimar Republic stored the results of a survey of German citizens on computer punch cards, the ancestors of the floppy disk. When the Nazis took power, they used this information to track down and eliminate minorities.¹⁷⁰ The Nazis did this again when they invaded Rumania, using the records of inhabitant's religion and addresses taken during a census to track down Jews and take them to concentration camps. The lesson is a simple one; powers innocently given to the government in good faith can be used to do terrible things.

The U.S. Government. In this country, the Fourth Amendment to the Constitution protects us from overzealous police action. The Fourth Amendment declares that "the right of the people in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated and no warrants shall issue, but upon probable cause." Any encryption regulation is subject to this requirement. Historically, however, the requirement that investigators obtain a warrant before initiating a search has been disregarded, circumvented, or grossly abused for political purposes.

The Fourth Amendment did not stop FBI surveillance of Martin Luther King, Jr.¹⁷¹ or from collecting files on opponents of the Vietnam War.¹⁷² Nor did it stop census data from being used to round up and inter Japanese-Americans during the Second World War.¹⁷³ And it could not stop Nixon's use of IRS files and unauthorized surveillance to