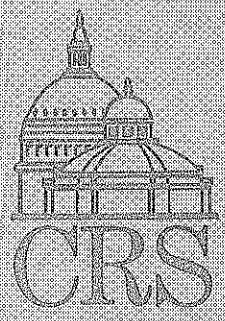
Order Code IB96039

CRS Issue Brief

Encryption Technology: Congressional Issues

Updated December 4, 2000

Richard M. Nunno
Resources, Science, and Industry Division



CONTENTS

SUMMARY

MOST RECENT DEVELOPMENTS

BACKGROUND AND ANALYSIS

Encryption, Computers, and Electronic Communications

Administration Policy: Gradual Relaxation of Rules
    Industry Reactions

Action in the 105th Congress

Action in the 106th Congress

Issues
    Key Recovery
    Export Restrictions
    Domestic Use

LEGISLATION

Encryption Technology: Congressional Issues

SUMMARY

The controversy over encryption concerns what access the government should have to encrypted stored computer data or electronic communications (voice and data, wired and wireless) for law enforcement and national security purposes.

Encryption and decryption are methods of using cryptography to protect the confidentiality of data and communications. When encrypted, a message only can be understood by someone with the key to decrypt it. Businesses and consumers want strong encryption products to protect their information, while the Clinton Administration wants to ensure the law enforcement community's ability to monitor undesirable activity in the digital age.

Until recently, the Administration promoted the use of strong encryption (greater than 56 bits) here and abroad, only if it had "key recovery" features where a "key recovery agent" holds a "spare key" to decrypt the information. The Administration wanted key recovery agents to make the decryption key available to authorized federal and state government entities. Privacy advocates argued that law enforcement entities would have too much access to private information.

Under this policy, the Administration was using the export control process to influence whether companies develop key recovery encryption products by making it easy to export products with key recovery, and difficult for those products without. There were no limits on domestic use or import of any type of encryption, so the Administration tried to influence what is available for domestic use through export controls since most companies do not want to create two products—one for U.S. use and another for export. In September 1997, however, FBI Director Louis Freeh raised the possibility of requiring encryption products manufactured in or imported into the United States to have key recovery features and opened the possibility that key recovery could be enabled by the manufacturer, not only the user. U.S. companies argued that U.S. export policies hurt their market share while helping foreign companies that are not subject to export restrictions. Many businesses and consumer groups agree that key recovery is desirable when keys are lost, stolen, or corrupted, but want market forces to drive the development of key recovery encryption products. They also object to government having any role in determining who can hold the keys.

All parties agreed that encryption is essential to the growth of electronic commerce and use of the Internet, but until September 1999, industry and privacy rights groups opposed the Administration's policy. In the 106th Congress, legislation was introduced intended to foster widespread use of the strongest encryption (H.R. 850, S. 798). While the Administration continued to oppose that legislation, H.R. 850 was marked up by five Committees, resulting in widely varying and, in places, opposing, legislation. S. 798 passed the Senate Commerce Committee and awaits further action.

In September 1999, the Administration announced plans to further relax its encryption export policy, and the rules for implementing that policy were issued by the Department of Commerce on January 14, 2000, after which, pressure from the industry (but not from privacy rights groups) to enact encryption legislation subsided.

MOST RECENT DEVELOPMENTS

On October 2, the National Institute for Standards and Technology announced its selection of a new Advanced Encryption Standard for federal agency use to protect unclassified information. The algorithm for the standard, known as Rijndael, was developed by Belgian scientists and will be made freely available for use by the private sector.

On July 17, the Administration announced further updates to its encryption policy to allow exports of any strength encryption products to the governments of European Union and eight additional countries. It also allows exports, without a technical review or reporting requirements, of encryption embedded in short-range wireless products (e.g., mobile phones, audio devices, cameras, and videos).

BACKGROUND AND ANALYSIS

Encryption, Computers, and Electronic Communications

Encryption and decryption are procedures for applying the science of cryptography to ensure the confidentiality of messages. Technically, the issue discussed here is cryptography policy, but since encryption is the most controversial application of cryptography, it is the term used popularly and herein. (There are other methods of using cryptography to protect confidentiality — steganography and "chaffing and winnowing" — but constraints on the length of this issue brief do not permit discussion of them.) Also, for a discussion of the specific issues regarding medical records privacy and security, see CRS Issue Brief IB98002, *Medical Records Confidentiality*, updated regularly.

Encrypting messages so they can be understood only by the intended recipient historically was the province of those protecting military secrets. The burgeoning use of computers and computer networks, including the Internet, now has focused attention on its value to a much broader segment of society. Government agencies seeking to protect data stored in their databases, businesses wanting to guard proprietary data, and consumers expecting electronic mail to be as private as first class mail, all want access to strong encryption products. Other users of electronic communications, for example cellular (wireless) phone users who expect calls to be as private as wireline calls, also are showing increased interest in encryption. While encryption is uncommon for telephone users today, the advent of digital telephone services (particularly Personal Communication Services, PCS, a digital form of cellular telephony) is expected to make encrypted voice and data communications over telephones more common.

Whether hardware- or software-based, an encryption product scrambles a message using mathematical algorithms. A corresponding key is needed to decrypt (unscramble) the message, and the key itself also may be encrypted. The algorithm is a series of digital numbers (bits), and the level of difficulty of breaking the code (its "strength") is usually represented by the number of bits in the key. (There are other factors that affect a key's strength, but in this debate, bit length is used as a benchmark.) Unencrypted data are referred to as "plaintext." Encrypted data are "ciphertext."

The National Institute of Standards and Technology (NIST), in conjunction with industry, developed an encryption standard using a 56-bit key in 1977. Called the Data Encryption Standard (DES), it is widely used today in the United States and abroad, often in an enhanced mode called "3-key triple DES" providing the equivalent of a 112- bit key. NIST is currently working to establish a new, stronger standard than DES referred to as the Advanced Encryption Standard (AES). The need for a stronger standard was underscored in 1997 when DES was broken (see below).

Encryption products are widely available today, including some that use 128-bit keys or more. Some 128-bit encryption software can be downloaded from the Internet. There are no limits on the strength of encryption products used in the United States, whether acquired here or imported. The only limits are on exports. This indirectly influences what is available domestically, however, since most U.S. companies are reluctant to develop two products, one for the U.S. market and another for export. For many years, reflecting the policies of the past three Administrations, the State Department did not allow general exports of encryption with more than 40-bit keys, except for banking and U.S.-owned subsidiaries (for a list of exceptions, see CRS Report 96-232). In December 1996, the Clinton Administration raised the limit to 56 bits for easily exportable encryption products that do not have key recovery features (see box), and removed bit length limits entirely for products with key recovery. Breaking a message encrypted with a 40-bit key by "brute-force" (trying every possible combination of bits until the correct one is found) is not considered difficult. In January 1997, a 40-bit key was broken in 3.5 hours. In general, for each bit added to the encryption key, the time required to break the key doubles. Thus it takes 2^{16} (65,536) times longer to break a 56-bit key than a 40-bit key. In July 1998, a group from the Electronic Freedom Foundation (an electronic privacy rights group) demonstrated (for less than $250,000) the vulnerability of 40- and 56-bit keys by using a network of nearly 100,000 PCs on the Internet that broke a 56-bit key in 22 hours, 15 minutes. The ability to break 128-bit encryption (considered strong encryption) has not yet been demonstrated in the commercial sector.

KEY RECOVERY AND KEY RECOVERY AGENTS

Once called "key escrow," key recovery means that when stored data or electronic communications are encrypted, a third party has a copy of the key needed to decrypt the information. The third party is called a key recovery agent (formerly a key escrow agent). Key recovery is widely regarded as useful in cases where a key is lost, stolen or corrupted. Most parties to the encryption debate agree that market forces will drive the development of key recovery-based encryption products for stored computer data because businesses and individuals will want to be sure they can get copies of keys in an emergency. It is less clear if market demands will drive key recovery systems for electronic communications.

The controversy is over government's attempt to "encourage" the development of key recovery-based products through the export control process, the government's role in determining who can serve as key recovery agents, and the extent to which law enforcement agencies could obtain the key if they suspect undesirable activity (terrorism, child pornography, and drug cartels are often cited as examples).

In May 1996, the National Research Council (NRC) released a comprehensive report entitled *Cryptography's Role in Securing the Information Society* (the "CRISIS" report). It stressed that national policy should make cryptography broadly available to all legitimate elements of society, promote continued economic growth and leadership of key U.S. industries, and ensure public safety and protection against foreign and domestic threats. Among the recommendations: key escrow is an unproven technology and the government should experiment with it and work with other nations, but not aggressively promote it now; export controls should be relaxed progressively, but not eliminated; and encryption policy issues can be debated adequately in public without relying upon classified information. The

report also recommended that no law should bar the manufacture, sale or use of any form of encryption within the United States; and government should promote information security in the private sector. The report underscored that utilization of strong encryption and law enforcement objectives can be mutually compatible.

Business and consumer groups consider 56-bit keys inadequate to ensure privacy and security. They oppose export encryption controls and requirements for key recovery features. They object to the government using the export process to force the development of key recovery encryption products, rather than allowing market forces to prevail, and to the government's role in determining who can serve as key recovery agents. These groups argue that strong encryption is needed, for example, to enhance the prospects for electronic commerce and other uses of computer networks. The willingness of consumers to buy goods via the Internet could be markedly affected by their beliefs as to whether credit card numbers will be secure. Businesses using computers for either internal or external communications need to ensure that competitors or other unauthorized parties cannot gain access to proprietary information. Privacy advocates argue that consumers should be assured that personal, medical and financial information transmitted by or stored in computers will be protected. They note that since 128-bit non-key recovery encryption is available worldwide either by downloading it from the Internet or buying it from foreign firms, the U.S. government already has lost control of influencing its availability. A 1997 survey conducted by Trusted Information Systems found 656 foreign encryption products available from 29 countries (in addition to 963 U.S. products). A 1998 report by the Economic Strategy Institute, *Finding the Key,* concluded that if the Administration's current policies remained in effect, the U.S. economy would lose $35-96 billion by 2002 in lost encryption product sales; slower growth in encryption-dependent industries; foregone cost savings and efficiency gains from the Internet, intranets, and extranets; and indirect effects throughout the economy.

In June 1999, a study conducted by George Washington University, titled the "Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations," found over 800 encryption products available from 35 foreign countries [http://www.seas.gwu.edu/seas/institutes/cpi]. At least 167 of those products were found to use strong encryption. Over 512 companies either manufacture or distribute cryptographic products (of quality comparable to U.S. products) in over 70 countries outside the United States. In June 1999, the Electronic Privacy Information Center (EPIC) produced its second annual report on the encryption policies of foreign nations and international organizations titled "Cryptography and Liberty," concluding that "in the vast majority of countries [both developed and developing] cryptography may be used, manufactured, and sold without restriction." On April 3, 2000, EPIC released its third annual international review of encryption policies, covering 135 countries. The report found the relaxation of export controls was continuing, but that law enforcement agencies were seeking new authority and new funding to gain access to private keys and personal communications.

PROPONENTS AND OPPONENTS OF ENCRYPTION EXPORT CONTROLS

Proponents include the Clinton Administration (notably the Department of Justice and the National Security Agency) and others who are concerned about the ability of terrorists and other criminal groups to conduct activities unmonitored if strong non-key recovery encryption is widely available.

Opponents include:

- computer hardware and software manufacturers who do not want to develop separate products for domestic and foreign markets and worry they will lose market share to foreign competitors who do not have to abide by such limits. They also are concerned that no one may buy encryption products for which the U.S. government can obtain the key.
- U.S. businesses that want to use the same computer systems they have in their home offices with their foreign clients; and
- privacy and consumer groups who want individuals to have access to the best encryption possible without regard to key recovery features.

Supporters of encryption export controls agree that strong encryption is needed but insist that law enforcement and national security concerns demand that, when authorized, the government be able to intercept and decrypt electronic communications or decrypt stored computer data where undesirable activity is suspected. Law enforcement and national security officials want to ensure their ability to access the plaintext of the information. The method most often discussed is to obtain the key needed to unscramble encrypted information from key recovery agents. Hence, they support the use of strong encryption products as long as they include key recovery features, and want to limit the development of strong non-key recovery products. While conceding some strong non-key recovery encryption products already are available, they claim use of these products is not widespread. They argue that while the U.S. government cannot prevent the availability of strong non-key recovery encryption, at least it can be restrained, and future generations of encryption products (with key recovery) will displace those now in use.

Although the publicity surrounding the encryption debate so far has centered on access to stored computer data, electronic communications are equally important to the law enforcement and national security communities. An Internet message, for example, is stored data when it resides on a server or an individual's computer, but it is an electronic communication while it is being transmitted between computers. The encryption export regulations apply to products for encrypting other electronic communications, not just those between computers. Telephones, whether wired or wireless (such as cellular phones), are also covered, for example. The 1994 Communications Assistance to Law Enforcement Act (CALEA, often called the "Digital Wiretap" Act, P.L. 103-414) requires telecommunications carriers to ensure their equipment permits the interception of any electronic communication by law enforcement officials. If the communication is encrypted, law enforcement agencies want to ensure they can decrypt it, too. (CALEA requires the telecommunications carrier to provide decrypted information if the carrier itself is responsible for the encryption, but not if the customer has encrypted it.)

Administration Policy: Gradual Relaxation of Rules

The Clinton Administration has always strongly supported arguments by law enforcement and national security agencies that the government must be able to gain access to the plaintext of encrypted electronic data and messages when undesirable activity is suspected. In addition to international criminal activity, the Administration (notably the FBI)

wants to be able to monitor domestic criminal activity. The Administration has always permitted use of any strength encryption, without a key recovery requirement, in the United States. Rather than attempting to change that policy directly, the Administration used the indirect route of export controls to influence what types of encryption products were available, both here and abroad.

Initially, the Clinton Administration sought to restrain the development of strong encryption products by prohibiting export of greater than 40-bit encryption (with a few exceptions). The Administration also tried several approaches to promote "voluntary" use of key recovery agents. In April 1993, the Administration released its "Clipper chip" policy requiring emplacement of special encryption computer chips (called Clipper, an encryption device used for unclassified but sensitive government communications) into new government equipment for voice communications, with two government agencies, NIST and the Department of Treasury, jointly serving as key escrow agents (each holds part of the key). The Administration implemented this policy in 1994 for sensitive but unclassified voice communications in the federal government through a Federal Information Processing Standard (FIPS) called the Escrowed Encryption Standard (EES, or FIPS-185). The Administration hoped that industry would accept the Clipper chip for its own use, but industry strongly objected to the key escrow provisions, particularly the fact that government agencies would hold the keys. In July 1994, the Administration agreed to work with the private sector to develop a "voluntary" key escrow system for data using "trusted third parties" as escrow agents instead of government agencies. This proposal was referred to by its detractors as "Clipper II."

Industry continued to object to the key escrow concept as well as the export controls, leading to the legislation discussed below. In May 1996, the Administration released a draft paper on encryption policy, followed by a July statement by Vice President Gore. Called "Clipper III" by its opponents, these documents outlined policy changes the Administration was considering. Among other things, the term "key recovery" replaced "key escrow" to emphasize the positive attributes of key escrow in providing a means to recover a key that is lost, stolen, or corrupted. Furthermore, "key escrow" had come to be identified with the concept of the government holding the key. Under the key recovery policy, a trusted third party or an organization itself can serve that function ("self escrow") with some restrictions.

On October 1, 1996, Vice President Gore announced the changes to the Administration's policy, to focus on the need for strong encryption, as long as it included key recovery features. The key recovery agent would be required to give the key to duly authorized law enforcement officials if undesirable activity is suspected (the three types most often cited are drug cartels, child pornographers, and terrorists). The associated executive order was signed November 15, and the Administration published an "interim final" regulation on December 30, to last two years, with the following details: continuation of no restrictions on domestic use or import of any encryption; no key length restrictions on export of encryption products if a key recovery system was used for that product; for 56-bit encryption products without key recovery systems, a one-time review was required before exporting the product, and within two years the exporter must have developed a key recovery system; export licenses were granted in 6-month increments to hold exporters to a timetable to ensure the key recovery systems were being developed (if not, the export license was not renewed); trusted parties served as key recovery agents, and in some cases, organizations were allowed to escrow keys themselves (self-escrow) if they met certain requirements; and commercial

encryption was removed from the Munitions List and responsibility for commercial encryption export licensing was transferred from the State Department to the Commerce Department, with the Department of Justice serving an advisory role in commercial encryption export decisions. Foreign governments would apply to U.S. courts to gain access to keys, as they do when seeking other types of evidence. During the next two years, the Commerce Department granted some waivers for banking and financial services.

On September 3, 1997, FBI Director Louis Freeh testified to the Senate Judiciary Committee that there was a need for domestic use restrictions on encryption products. Following that testimony, the existence of legislation proposed by the Administration to impose domestic use restrictions became widely known among congressional and industry groups. Vice President Gore later stated that Freeh's comments reflected the FBI's view, but did not indicate a change in Administration policy. The House Intelligence Committee, however, later approved an amendment to legislation similar to Freeh's position about the need for key recovery to be built into encryption products.

In March 1998, Vice President Gore wrote to Senator Daschle restating the Administration's desire for a "balanced approach" to encryption policy and seeking to "produce cooperative solutions, rather than seeking to legislate domestic controls." The discussions would also enable additional steps to relax export controls on encryption products. On April 15, Secretary of Commerce Daley announced the release of a new report on electronic commerce wherein he said that although the Administration's policy was the right one, its implementation was a failure. He urged both industry and government to strive harder to reach consensus on the issue. In April 1998, Undersecretary of Commerce for the Bureau of Export Administration (BXA) Reinsch commented at a Congressional Internet Caucus meeting that the Administration was no longer looking for a legislative solution to the encryption issue.

In July 1998, the Administration declassified two security algorithms used in the Clipper chip. In September 1998 it announced plans to allow the export of 56-bit encryption products without requiring provisions for key recovery, after a one-time review, to all users outside seven "terrorist countries" (Cuba, Iran, Iraq, Libya, North Korea, Syria, and Sudan). Export of encryption products of any strength was permitted to 46 designated countries if key recovery or access to plaintext is provided to a third party. The Administration also supported an FBI proposal to establish a technical support center to help law enforcement keep abreast of encryption technologies. In December 1998, the BXA released interim rules to implement the Administration's export control policy initiative. The rules allowed for the export of encryption commodities and software to U.S. companies or subsidiaries in the finance, insurance, health-care and medical end-users, and electronic commerce industries.

In September 1999, the Administration announced its new encryption export policy, to make encryption products of any key length, after a technical review, exportable without a license to users in any country except seven "terrorist countries". Regulations implementing the Administration's new encryption export policy were issued by the BXA on January 14, 2000. According to the new rules, retail encryption commodities and software of any key length can be exported without a license to any non-government end user in any country except the seven state supporters of terrorism, and can be re-exported to anyone (including Internet and telecommunications service providers). Exports previously allowed only for a company's internal use can now be used for communication with other firms, supply chains,

and customers. Exports to government end-users still require a license. Exporters must report to BXA on where the encryption product is exported, and BXA will determine whether products qualify as retail by reviewing their functionality, sales volume, and distribution methods. In addition, if source code (computer language instructions written by programmers) is made publicly available (under "open source" policies) and no royalty is charged for its use, the code is not subject to export restrictions, a provision that was not included in an earlier draft and was the source of criticism by industry and privacy rights groups.

Industry Reactions

Most participants in the debate agreed that market forces will lead to the development of key recovery-based encryption products for stored data because companies and individuals will want to be able to replace lost, stolen or corrupted keys. The debate was over the government's role in "encouraging" the development of key recovery products through export regulations and the access government has to the keys. Also of concern was the government's inclusion of other electronic communications.

While computer companies continued to argue against the Administration's policy, some also developed key recovery products to satisfy the policy. A group of companies formed the Key Recovery Alliance [http://www.kra.org] in 1996 to identify barriers to the development of marketable key recovery products. On March 4, 1998, a group of more than 100 companies and organizations (some also members of the Key Recovery Alliance) formed the Americans for Computer Privacy (ACP) coalition [http://www.computerprivacy.org] to lobby for enabling the use of strong encryption, against export controls on strong encryption, and against mandatory key recovery. Among the members are America On Line, Microsoft, Sybase, the National Rifle Association, the Law Enforcement Alliance of America, and the Business Software Alliance.

In March 1998, Network Associates announced that it had arranged for a Swiss company to develop its own software product using specifications in a book by Philip Zimmerman, the creator of Pretty Good Privacy (PGP). Network Associates bought Mr. Zimmerman's company in 1997. PGP is a 128-bit encryption product that does not have key recovery and hence could not be exported under the current regulations. (An older version is available via the Internet, however, which sparked a multi-year Justice Department investigation of Mr. Zimmerman that resulted in no action against him). Since the book may be exported, and the Swiss company received no technical assistance from Network Associates, the company believes no laws were broken. The Swiss product was sold by a Dutch firm under the PGP name. Opponents of encryption controls pointed to this as evidence that the U.S. government cannot control the spread of non-key recovery encryption.

In July 1998, as a possible compromise to the Administration, a group of software companies announced plans to develop a product, "private doorbell", to capture data that could be given to law enforcement before it is encrypted and sent over the Internet. While industry groups approved of the Administration's encryption export policy, they argued that 56-bit encryption had been broken and that stronger encryption was necessary. Furthermore, the Department of Commerce's rules could render the policy ineffective in increasing their ability to export encryption products. Privacy rights groups argued that while the new policy

may help big companies, it would not increase the availability or use of 56-bit or stronger encryption by individual users of Internet communications.

While the computer industry is satisfied with the latest rules, some privacy rights groups (including the American Civil Liberties Union, the Electronic Frontier Foundation, and the Electronic Privacy Information Center) argue that the remaining ambiguities in the rules make encryption technology overly cumbersome for individuals to use. Because the regulations could be reversed by a future Administration, these groups still advocate the passage of legislation to codify the changes in U.S. encryption policy.

Action in the 105th Congress

Three bills in the House and four in the Senate concerning encryption were introduced in the 105th Congress; none were enacted, although one (H.R. 1903) passed the House. Three (H.R. 695, S. 376, and S. 377) were versions of bills considered in the 104th Congress, generally favoring relaxed encryption export controls. Four new bills were also introduced. S. 909 reflected a philosophy closer to that of the Clinton Administration than the three previous bills. H.R. 1903 focused broadly on computer security issues and the role of NIST. H.R. 1964 focused broadly on computer privacy and security issues. S. 2067 was generally viewed as pro-industry and pro-privacy. Hearings were held by six House committees (Commerce, International Relations, Intelligence, Judiciary, National Security, and Science) and two Senate committees (Judiciary; and Commerce, Science, and Transportation).

The Security and Freedom Through Encryption (SAFE) Act (H.R. 695, Goodlatte), as introduced, sought to relax export controls on encryption, although versions of H.R. 695 as reported from various committees had substantially different provisions. The bill was eventually considered by the Committees on Judiciary, International Relations, Commerce, National Security, and Intelligence. Amendments adopted by the latter two committees reversed some of the provisions of the original bill by maintaining or increasing restrictions on export controls of encryption. The Rules Committee did not take action on the bills.

The Encrypted Communication Privacy Act of 1997 (S. 376, Leahy) prohibited mandatory use of key recovery but allowed law enforcement to access the key under court order if key recovery is used; codified existing domestic use policy; gave the Secretary of Commerce exclusive jurisdiction over commercial encryption exports; liberalized export controls; made it a crime to use encryption to obstruct justice; and established liability protection and penalties for "key holders." The bill also established procedures for foreign governments to access keys or decryption assistance.

The Promotion of Commerce On-Line in the Digital Era (PRO-CODE) Act of 1997 (S. 377, Burns) prohibited mandatory key recovery and established an Information Security Board as a forum to foster communication and coordination between industry and government. The bill also codified existing domestic use policy and gives the Secretary of Commerce exclusive jurisdiction over commercial encryption exports. It liberalized export controls but required the publisher or manufacturer of encryption software or hardware to report to the Secretary of Commerce within 30 days after exporting a product on the product's encryption capabilities. The report would have included the same information

required under the December 30, 1996 regulations, but would be provided after export instead of as a condition of obtaining a license.

The Secure Public Networks Act (S. 909, McCain et. al.) codified existing domestic use policy; established penalties for use of encryption in commission of a crime; encouraged but did not require use of key recovery; established procedures for government approval of key recovery agents and certificate authorities; required key recovery agents, whether or not registered by the government, to disclose recovery information to lawfully authorized federal or state government entities; provided liability protection for key recovery agents acting pursuant to the Act; permitted export of 56-bit encryption products without key recovery if they meet certain conditions; permitted export of any strength encryption product if it is based on a qualified key recovery system and meets certain other conditions; and allowed the President to waive provisions of the bill for national security or domestic safety and security reasons. During and after markup, the committee adopted amendments establishing an Encryption Export Advisory Board (EEAB) with four government (CIA, FBI, NSA and the White House) and eight industry representatives to make recommendations on whether export exemptions should be granted for non-key recovery products stronger than 56-bits. The committee ordered the bill reported, but the report was never filed.

The Senate Judiciary Committee requested sequential referral of S. 909, and held a hearing on July 9, 1997 where FBI Director Louis Freeh expressed reservations about the bill because it allowed widespread use of strong encryption within the United States regardless of whether it has key recovery. Freeh amplified his concerns at a September 3 hearing before the Subcommittee on Technology, Terrorism, and Government Information. He stated that he wanted U.S. manufacturers to be required to build key recovery into encryption products, and that imported encryption products also be required to include key recovery. He further stated that achieving the goal of immediate lawful decryption "could be done in a mandatory manner. It could be done in an involuntary manner. ..." He later added that he thought legislation should first include the requirement that key recovery be built into encryption products and "then take up the more complex discussion about how that's enabled...." He also stated that Internet service providers should be required to be able to decrypt communications immediately.

The Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY) Act (S. 2067, Ashcroft, et. al.) prohibited federal or state agencies from linking the use of encryption for authentication or identification to the use of encryption for confidentiality purposes; required that the use of encryption products be voluntary and market-driven; outlined procedures for U.S. and foreign law enforcement agencies to access decryption keys or assistance in decrypting electronic communications or stored data; established a National Electronic Technologies (NET) Center in the Department of Justice to help law enforcement keep pace with encryption technology; made the use of encryption to obstruct justice a crime; established an Encryption Export Advisory Board to determine whether comparable foreign products are commercially available; maintained the President's authority to prohibit export of encryption products to countries that support international terrorism or to impose embargoes on exports to or imports from a specific country; made electronic records in networked storage be treated in law as though the record had remained in the possession of the person who created the record; and set the circumstances under which the government may require a mobile electronic communication service to reveal the real-time

physical location of a subscriber, and may obtain information from pen register and trap and trace devices.

The Computer Security Enhancement Act (H.R. 1903, Sensenbrenner) amended and updated the Computer Security Act of 1987, enhancing the role of the National Institute of Standards and Technology (NIST). As passed by the House (H.Rept. 105-243), the bill required NIST to promote the use of commercial-off-the-shelf encryption products by civilian government agencies; clarified that NIST standards and guidelines are not intended as restrictions on the production or use of encryption by the private sector; provided funding for computer security fellowships at NIST; and required the National Research Council to conduct a study of public key infrastructures. A section requiring NIST to develop standardized tests and procedures to evaluate the strength of foreign encryption products was removed before passage. The bill passed the House and was reported without amendment by the Senate Commerce Committee October 13, 1998 (S.Rept. 105-412).

The Communications Privacy and Consumer Empowerment Act (H.R. 1964, Markey) covered a range of computer privacy and security issues. With regard to encryption, the bill codified existing domestic use policy, prohibited the government (federal or state) from conditioning the issuance of certificates of authentication or certificates of authority upon use of key recovery systems, and prohibited the government (federal or state) from establishing a licensing, labeling or other regulatory scheme that requires key escrow as a condition of licensing or regulatory approval. The bill also required the National Telecommunications and Information Administration (NTIA) to conduct a study on, inter alia, how data security issues affect electronic commerce, including identification of generally available technologies (including encryption) for improving data security.

Action in the 106th Congress

On February 25, 1999, Representative Goodlatte introduced a new version of SAFE (H.R. 850), similar to the bill introduced in the 105th Congress, with a new provision directing the Attorney General to compile examples in which encryption has interfered with law enforcement. The bill was reported by the Judiciary Committee on April 27, and was referred jointly and sequentially to Committees on International Relations, Commerce, Armed Services, and Intelligence. Hearings were held by the Committees on Commerce (May 5 and 25), International Relations (May 18) and Intelligence (June 9 and July 14), Armed Services (July 1 and 13), . The bill has gained 257 co-sponsors, with a majority of both Republican and Democratic leadership. The bill was reported (amended) by the Committee on Commerce. (H.Rept. 106-117, Part II) on July 2, and by the remaining three committees (parts III, IV, and V) on July 23.

The five versions of H.R.850 differ significantly. The versions passed by the Committees on the Judiciary, Commerce, and International Relations codify the regulations for unrestricted domestic use and sale of encryption, prohibit the government from mandating key escrow practices for the public, and liberalize the controls governing the export of strong encryption. One of the amendments passed by the Commerce Committee made it a crime to fail to decrypt information upon court orders, raising opposition from privacy rights advocates. The Armed Services and Intelligence Committee versions, in contrast, have minimal or no mention of domestic use of encryption, and increase the authority of the

President in restricting the controls governing the export of strong encryption. All of the bills, except for the version by the Armed Services Committee, establish criminal penalties for the use of encryption in the furtherance of a criminal act. The Intelligence Committee bill, however, provides greater details than the others for criminalizing the use of encryption in a criminal act. In addition, each Committee added provisions for specific agencies and circumstances. For example, the Commerce Committee established a National Electronic Technologies (NET) Center in the Department of Commerce to promote the exchange of information regarding data security techniques and technologies, and the International Relations Committee directed the Secretary of Commerce to consult with the Attorney General, the Federal Bureau of Investigation, and the Drug Enforcement Administration before approving any license to export encryption products to any country identified as being a major drug producer. The Intelligence Committee bill authorizes appropriations for the Technical Support Center, at the FBI. The bill was sent to the House Rules Committee for further action on July 23, 1999.

In the Senate, On April 14, 1999, Senators McCain, Burns, Wyden, and Leahy introduced S. 798, the Promote Reliable Transactions to Encourage Commerce and Trade (PROTECT) Act. The bill would immediately raise the maximum exportable key length of encryption products to 64 bits; S. 798 also sets a deadline of January 1, 2002 for the federal adoption of the Advanced Encryption Standard (which uses a 128 bit key length) and allows the export of products employing AES at that date. S.798 allows the export of strong (greater than 64 bit) encryption products with key recovery features, as well as the export of strong encryption products to "legitimate and responsible entities," including publicly traded firms, U.S. corporate subsidiaries or affiliates, firms required by law to maintain plaintext records, and others. S.798 does not contain criminal provisions for the use of encryption in the furtherance of a crime (unlike H.R.850), and prohibits domestic controls and mandatory plaintext access. The Senate Commerce Committee held a hearing on the bill on June 10. The Senate Commerce Committee approved S. 798 on June 23, 1999.

Deep divisions remain between those who oppose liberalizing encryption policy and those who advocate it. While the computer industry, and privacy and consumer advocacy groups generally favor both bills, H.R. 850 is considered more pro-industry because of its greater liberalization of encryption export controls. The Administration remains opposed to both bills, arguing that the current export restrictions are necessary to prevent the use of encryption by undesirable groups, and has increased its efforts to maintain the status quo on encryption policy. Reaching a compromise on some of the differences (such as key escrow and export policies) may be a difficult task. In addition, on July 27, 1999, Representative Goss introduced two more bills on encryption policy: H.R. 2616 (which reflects House Intelligence Committee mark-up of H.R. 850), and H.R. 2617 (which proposes tax incentives for the nation's encryption software manufacturers to develop products with key recovery). The prospects for enacting legislation are further complicated by a possible veto by President Clinton if the final bill passed by Congress is not supported by officials in the Defense and Justice Departments.

Three other bills have been introduced containing provisions regarding encryption. On April 21, 1999, Senator Leahy introduced S. 854, which includes provisions that promote the use of encryption by (1) prohibiting government requirements for non-federal use of key recovery or plaintext access practices, (2) prohibiting federal agencies from requiring non-federal entities to use specific encryption products to receive services, (3) prohibiting federal

encryption products that interact with commercial systems from interfering with the encryption capabilities of the commercial products, and (4) prohibiting the disclosure of decryption assistance to foreign governments without a court order. The bill was referred to the Committee on the Judiciary. On June 9, 1999, Representative Sensenbrenner introduced H.R. 2086, which includes a provision directing the National Science Foundation to undertake a study comparing the availability of encryption technologies in foreign countries to those subject to U.S. export restrictions. On July 1, 1999, Representative Sensenbrenner introduced H.R. 2413, which contains provisions for establishment of a public key management infrastructure and encryption standards for federal computers.

On September 21, 1999, the President sent to Congress proposed legislation that would ensure that law enforcement maintains its ability to access decryption information stored with third parties, and is allowed to withhold information in courtrooms on its techniques used in decryption. The bill would also authorize $80 million over four years for the FBI Technical Support Center, which will serve as a technical resource in responding to the use of encryption by criminals. To date, no Member has introduced that legislation.

Issues

Key Recovery

Key recovery is the fundamental tenet of the Clinton Administration policy. The Administration wants law enforcement access to keys for encrypted data stored by computers, transmitted between computers, or other types of electronic communications. Not only does the Administration view this as critical for U.S. users, but it seeks creation of a global key management infrastructure (KMI, now referred to as public key infrastructure, or PKI) to ensure confidentiality for the growth of global electronic commerce, and monitoring undesirable activity (by terrorists, drug cartels, or child pornographers, for example).

Many opponents of encryption controls agree that key recovery has advantages for recovering a lost, stolen, or corrupted key, but believe market forces will drive the development of a KMI for stored computer data without government involvement. Less likely is a market-driven demand for key recovery products for electronic communications. In any case, opponents of controls insist that the government should have no role in choosing who holds the keys. They fear the government will have unfettered access to private files and communications, though the Clinton Administration stresses that proper legal authorization will be required. Liability protection for proper release of keys, and penalties for improper use or release of keys, is an important aspect of Administration policy.

Questions about technical vulnerabilities that could be introduced if key recovery is incorporated into computer systems were raised in a report (updated June 1998), *The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption,* by an ad hoc group of cryptographers and computer scientists. They concluded that key recovery "introduces a new and vulnerable path to the unauthorized recovery of data" and the "massive deployment of key-recovery-based infrastructures to meet law enforcement's specifications will require significant sacrifices in security and convenience and substantially increased costs...."

The Administration acknowledges that global agreement on key recovery and KMI policy is essential to its policy and has been working with the Organization for Economic Cooperation and Development (OECD) to develop guidelines for a global KMI. In 1997, the OECD released those guidelines, which state that "national cryptography policies *may* allow lawful access to plaintext, or cryptographic keys, or encrypted data" (emphasis added). Hence, OECD neither endorsed nor rejected the concept of law enforcement access to decryption keys. The European Commission published a communication in October 1997 that noted the need for strong encryption to advance electronic commerce and expressed strong reservations about regulating encryption (by requiring key recovery, for example). Since then, Canada, Finland, Germany, France, and Taiwan have announced a relaxation or elimination of their key recovery laws. Lacking international consensus, many believe it is unlikely that mandated key recovery will survive.

Export Restrictions

Using the export process to influence the type of encryption products that are available in the United States and abroad is one strategy of the Administration's policy. The Administration points to threats to national security and public safety that would arise if criminals and terrorists used encryption that the U.S. government could not decrypt. Administration representatives argue that NSA, for example, has been able to thwart criminals and terrorists because NSA intercepted communications in time; if those communications had been encrypted with strong encryption, their task would have been much more difficult. NSA opposes passing a law that does not require companies to notify the government of what encryption products are being exported and to whom. Others point to difficulties in stopping future attacks in an era when terrorists could use strong encryption.

Opponents of the Administration's policy counter that the United States, through export controls, cannot prevent access to strong non-key recovery encryption by criminals and terrorists because it is already available elsewhere in the world. They further point out that the current policy of no restrictions on domestic use or import of encryption means that domestic threats would not be affected.

Until its September 1999 announcement, the Administration was using the export process to encourage companies to develop products with key recovery features. There were no limits on the strength of encryption products that can be exported if they include key recovery. Opponents of export controls object to the government mandating the use of key recovery, arguing that foreign companies are not bound by such restrictions. They argue that customers who do not want U.S. law enforcement or national security agencies having access to decryption keys will buy encryption products from foreign suppliers. They insist that the U.S. government cannot control the availability of strong non-key recovery encryption products, since they already can be procured from foreign suppliers, or downloaded from the Internet. They assert U.S. policies simply ensure that U.S. companies will lose market share to foreign competitors and will not achieve the overall objective of assuring law enforcement access to encrypted information of criminal groups. They point out that drug cartels, for example, could develop their own encryption products rather than buying commercially available products that would allow governments to access the keys.

Proponents of export controls concede that some criminal groups may develop their own encryption, but insist that at some point they will have to interact with mainstream companies

(such as banks or airlines). If the mainstream companies are using key recovery-based systems, this would provide an opportunity for law enforcement to access at least some of the groups' activities. They also point out that even though law enforcement agencies have been allowed to tap telephone lines for decades, criminals still use telephones because the infrastructure is already in place, easily used, and less costly than building an alternative system for their own use. As for foreign competition, proponents argue that although some strong non-key recovery products are available from the Internet or foreign suppliers, they are not widely used and some are not as strong as their advertisements claim.

Some cases involving encryption export controls have been the basis for legal action. One involves University of Illinois Professor Daniel Bernstein and his attempts to publish, both in print and on the Internet, the source code for his Snuffle encryption algorithm. The government argued that the export required a license under the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) through which AECA is implemented. On April 15, 1996, U.S. District Judge Marilyn Patel ruled that computer source code is "speech" and protected under the Constitution. On December 18, she further ruled that ITAR represents an unconstitutional prior restraint on free speech. Following the December 30, 1996 shift in jurisdiction over commercial export products from the State Department to the Commerce Department, Bernstein's lawyers asked her to review the new regulations. On August 25, 1997 she ruled that the new regulations also violate the First Amendment. On June 21, 1999, the Department of Justice filed a petition with a federal appeals court for reconsideration in the Bernstein case, which on May 6 upheld a ruling that encryption source code is scientific expression protected by the First Amendment.

An opposite ruling was made in March 1996 by Judge Charles Richey in a case involving Philip Karn. Mr. Karn was denied permission to export source code on diskette even though the source code had been published in a book and hence was in the public domain. The State Department designated the diskette as a "defense article" under AECA and denied its export. Judge Richey dismissed the complaint because the AECA does not permit judicial review of what is designated by the President as a "defense article." Mr. Karn appealed the ruling, but by the time the appeal was heard in January 1997, the export regulations had changed so the case was remanded back to DC District Court. On July 7, 1998, U.S. District Judge James Gwin ruled that an individual could not challenge encryption export restrictions on the grounds that they abridge his right to free speech on the Internet.

Domestic Use

The focus of the encryption debate has at times shifted to include potential changes to domestic use policy. Current U.S. policy allows any type of encryption to be used in or imported into the United States. Administration concerns that attempting to change this policy would be unsuccessful was a factor in its choice of using export controls to influence what encryption products are available for domestic use. FBI Director Freeh's testimony to the Senate Judiciary Committee on September 3, 1997 heralded a shift in the debate toward the possibility of requiring that key recovery be built into products manufactured in or imported into the United States, and possibly enabled by the manufacturer, not only the user. The Administration's policy, however, has not changed on this issue.

In September 1999, questions were raised over the discovery of a software element, labeled NSAKey, in the security code of the Microsoft Windows operating system. Microsoft

stated that the element was a back-up used for authentication of encryption components if the first key is damaged. Some question whether the key might enable the National Security Agency (NSA) to gain access to Windows operating systems. While it is unlikely that Microsoft would collaborate surreptitiously with NSA, the dispute highlights the level of tension between industry and privacy rights groups over key recovery practices.

LEGISLATION

H.R. 850 (Goodlatte)

Security and Freedom Through Encryption (SAFE) Act. Similar to H.R. 695 from 105th Congress, with changes including creating criminal penalties for the use of encryption to conceal criminal conduct, and directing the Attorney General to compile examples in which encryption has interfered with law enforcement. Introduced February 25, 1999; referred to Committees on Judiciary and on International Relations; referred to Subcommittee on Courts and Intellectual Property March 3; Committee mark-up March 24; reported by Committee (H.Rept. 106-117, Part I) April 27 without amendment; referred jointly and sequentially to Committees on Armed Services, Commerce, and Intelligence, for a period ending not later than July 2 (later extended to July 23); reported by Committees on Commerce June 23 (H.Rept.106-117, Part II); International Relations July 19 (H.Rept. 106-117, Part III); Armed Services and Intelligence July 23 (Parts IV and V). Placed on the Union Calendar July 23.

H.R. 2086 (Sensenbrenner)

Networking and Information Technology Research and Development Act. Contains provision for an NSF study comparing availability of encryption technologies in foreign countries to such technologies subject to export restrictions in the United States. Introduced June 9, 1999; reported (amended) by the Committee on Science (H.Rept. 106-472, Part I) November 16; referred to Committee on Ways and Means.

H.R. 2413 (Sensenbrenner)

Computer Security Enhancement Act. Contains provisions for establishment of a public Key Management Infrastructure and encryption standards for federal computers. Introduced July 1, 1999; referred to Committee on Science.

S. 798 (McCain)

Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999. Intended to promote electronic commerce by encouraging and facilitating the use of encryption in interstate commerce consistent with the protection of national security. Introduced April 14, 1999; referred to Committee on Commerce, Science, and Transportation; ordered to be reported June 23 without amendment; report filed August 5 (S.Rept. 106-142).

S. 854 (Leahy)

Electronic Rights for the 21st Century Act. Intended to protect the privacy and constitutional rights of Americans, to establish standards and procedures regarding law enforcement access to location information, decryption assistance for encrypted communications and stored electronic information, and other private information, and to affirm the rights of Americans to use and sell encryption products as a tool for protecting their online privacy. Introduced April 21, 1999; referred to Committee on the Judiciary.