

Encryption Exportation Restrictions:
Balancing National Security and
Economic Interests

John K. Rhoads
IEEE and WISE 98
August 1998

Table of Contents

ABOUT THE AUTHOR	3
WISE	3
ACKNOWLEDGMENTS	3
EXECUTIVE SUMMARY	4
INTRODUCTION	5
CRYPTOGRAPHY AND ENCRYPTION.....	5
KEY CRACKING TIME.....	5
THE IMPORTANCE OF ENCRYPTION	6
CURRENT US REGULATIONS	7
MOST RECENT DOMESTIC DEVELOPMENTS.....	8
THE NATIONAL SECURITY THREAT	9
NEEDS FOR ACCESS TO ENCRYPTED DATA	9
POLICY OBJECTIVES.....	10
ECONOMIC COMPETITIVENESS AND PRIVACY	10
DAMAGE TO US DEVELOPMENT OF INFORMATION TECHNOLOGY	10
CHALLENGES IN THE COURTS	11
POLICY OBJECTIVES.....	12
ASSESSMENT	12
FOREIGN POLICY CONSIDERATIONS	12
EFFECTIVENESS OF CURRENT POLICY ON NATIONAL SECURITY	13
EFFECT OF CURRENT POLICY ON CIVIL LIBERTIES AND PRIVACY	14
EFFECT OF CURRENT POLICY ON BUSINESS.....	14
POLICY OPTIONS AND RECOMMENDATIONS	16
EXPORT CONTROL OPTIONS	16
RECOMMENDATIONS ON PENDING LEGISLATION	16
APPENDIX	17
PENDING LEGISLATION.....	18
<i>H.R. 695: Security and Freedom Through Encryption (SAFE)</i>	18
<i>S. 376: Encrypted Communications Privacy Act (ECPA)</i>	20
<i>S. 377: Promotion of Commerce On-Line in the Digital Era (PRO-CODE)</i>	20
<i>S. 909: the Secure Public networks Act</i>	20
<i>S. 2067: Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY) Act</i>	22
<i>H.R. 1903: The Computer Security Enhancement Act of 1997</i>	23
<i>H.R. 1964: Communications Privacy and Consumer Empowerment Act</i>	23
SOME ORGANIZATIONS ADVOCATING PROLIFERATION OF STRONG ENCRYPTION TECHNOLOGY.....	24
SOME ORGANIZATIONS OPPOSING THE PROLIFERATION OF STRONG ENCRYPTION TECHNOLOGY.....	25

About the Author

John Rhoads is a senior in the Electrical Engineering Department of Tulane University. This paper is the result of his research conducted during the Washington Internships of Students of Engineering (WISE) program of 1998. His internship was sponsored by the Institute of Electrical and Electronics Engineers (IEEE).

WISE

The Washington Internships for Students of Engineering is a ten-week program for outstanding engineering students who have completed their junior year and display evidence of leadership skills and interest in public policy. The students spend the summer in Washington, DC, learning how engineers contribute to public policy decisions on complex technological matters. Through frequent meetings and discussions with government officials and other policy-makers, students examine a variety of public policy issues. Each student completes a paper that analyzes specific engineering public policy issues of concern to the sponsoring society. For information about the WISE program, contact WISE, Attn: Anne Hickox, 400 Commonwealth Dr., Warrendale, PA 15096-0001.

Acknowledgments

The author would like to express his thanks to the members and officers of IEEE and IEEE-USA for their support of the WISE program. It is the author's opinion that programs such as WISE provide an education unavailable in academia. Through their support of the WISE program, IEEE-USA and the other sponsoring societies have furthered the education of many future engineers.

Thanks also go to the administrators of the WISE program. In particular, Dr. Wolf Yeigh, 1998's faculty-member-in-residence, for his advice and guidance during the WISE program. Special thanks to the IEEE-USA WISE mentor, Chris Brantley, for his support, which was invaluable in the research and writing of this paper.

Encryption Export Controls: Balancing National Security and Economic Interests

Executive Summary

The controversy over encryption exportation restrictions centers on what access intelligence and law enforcement agencies should have to encrypted electronic communications. The Clinton administration, the intelligence community, and numerous security and law enforcement organizations support the lawful use of strong encryption so long as it features a “key recovery mechanism,” allowing law enforcement agencies to quickly and clandestinely gain access to the encrypted data communications.

Opposing government intervention in the development and spread of strong encryption technologies are the many industries that rely on electronic communications, who stand to lose billions of dollars due to the costs incurred as a result of current restrictions. If restrictions continue, domestic producers of products incorporating encryption mechanisms will lose sales to foreign competitors, who are not subject to the same government restrictions. Also opposing restrictions are privacy and civil liberty advocates, who worry that law enforcement agencies would have easy access to private, personal information.

All parties involved agree that encryption is essential to the growth of electronic communications and commerce. There have been seven bills on encryption introduced in the 105th Congress, and hearings have been held in several congressional committees. Currently, strong encryption products which do not incorporate “key recovery mechanisms” are unlawful to export.

The current restrictions have had little impact in limiting worldwide availability of strong encryption. Most foreign countries are unwilling to adopt US plans to restrict the sale of encryption products. In the absence of a global plan to control the proliferation of strong non-key encryption products, export restrictions cost US businesses billions of dollars and jeopardizes future US development and leadership in the quickly expanding information technology industry. The US government should abolish current export restrictions, which have compromised domestic security and economic interests. In the absence of global support, the US government cannot expect to influence the proliferation of non-key recovery encryption products.

Introduction

Cryptography and Encryption

Encryption is a method of applying cryptography to protect the confidentiality of communications. An encrypted message can only be decrypted into understandable “plain text” format by using the correct key. Historically, encryption has been used mainly to protect military communications. More recently, the widespread use of electronic communications in computer networks has expanded the use of encryption products to a much broader market.

Both hardware and software can be used to encrypt electronic data. In electronic communications, a message is transferred through a long, binary string of 1s and 0s, which represent different letters and characters. An encryption product uses a mathematical algorithm, which reorders, rearranges, and changes the stream of information in a systematic way. Through this process, a message is encrypted into unreadable “ciphertext.” The ciphertext message can then be decrypted into readable, plain text format by knowing how it was scrambled. By finding and using the correct key, a computer can correctly decrypt an encrypted message.

The strength of an encryption mechanism can be measured by the difficulty of finding the correct key to a specific encryption algorithm. The strength is mostly determined by the number of binary numbers, or bits in the key. The greater the number of bits in a key, the more possible combinations. It should be understood that a 57-bit encryption product has twice as many possible keys as a 56-bit encryption product. There are many other factors in determining the strength of an encryption mechanism, but bit length is the most crucial and the easiest to quantify.

Key Cracking Time

The time it takes to crack an encryption mechanism depends on the strength of the encryption mechanism used. Greater computing power and knowledge of the encryption scheme greatly decreases key cracking time. If nothing is known of the encryption mechanism used, it is possible to find the correct key by trying all possible combinations. This approach is referred to as the “brute strength” method.

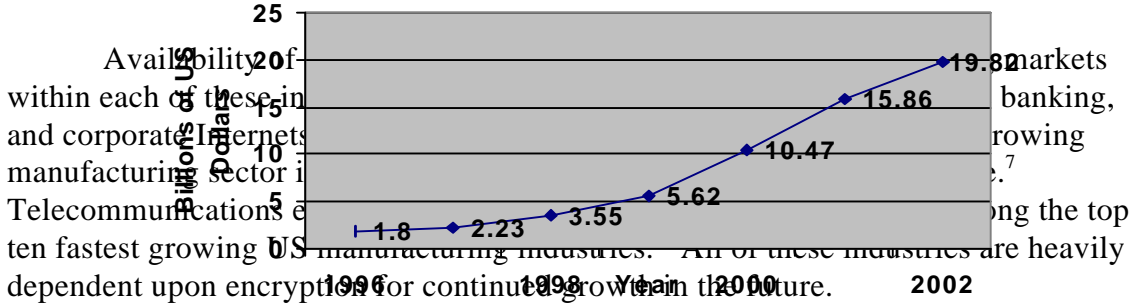
40-bit encryption mechanisms can be broken in a matter of hours by the brute strength method if enough computing power is used. Very recently, a popular 56-bit encryption scheme developed by NIST called the Data Encryption Standard (DES) was broken in less than 3 days using a specially built machine costing less than \$250,000.¹ Currently, there is no public evidence that any 128-bit encryption mechanisms have been broken by the brute strength method, but it should be expected that stronger encryption mechanisms will be needed as computing power continues to increase.

¹ Electronic Frontier Foundation, “EFF Builds DES Cracker that Proves that Data Encryption Standard is Insecure,” July 17, 1998, <<http://www.eff.org/descracker/>>.

The Importance of Encryption

The annual worldwide market for encryption products in 1996 was estimated at \$1.8 billion, with the US market accounting for nearly half of the global market.² Over the past five years, the encryption industry has posted a compound annual growth rate of 29%.³ Annual growth in the industry is projected to surpass 59% over the next five years, producing a worldwide market worth \$20 billion in 2002.⁴ The economic importance of encryption is most closely connected to the growth of six major US industries, including computer software and networking equipment, telecommunication services, telecommunications equipment, computers and peripherals, electronic commerce, and financial services.⁵ These six industries are expected to continue to experience phenomenal annual growth rates, and collectively generate nearly \$1 trillion in annual revenues.⁶

Figure 1: A Sector Poised for Explosive Growth: Encryption Revenue Forecast
Source: Economic Strategy Institute



Encryption technology is already heavily utilized in many of the most popular hardware and software products, including Ethernet and Internet navigators and routers, cellular phones, and wireless communications products. Financial institutions are currently the largest users of encryption products, making use of them to protect financial information and transactions. The heavy use of encryption in financial, voice, and data communications guarantees that there will continue to be an increasing global demand for secure electronic communications.

² US Department of Commerce, US Industry and Trade outlook 1998, pg III-1. The Center for National Security Policy estimates that the market is valued at only \$500 million [Center for National Security Policy, “Breaking the Code on the Encryption Debate: National Security Interests Are Being Jeopardized,” No. 97-D 88, p. 1 <<http://www.security-policy.org/papers/97-D88.htm>>]. A figure of \$3.3 billion comes from US Department of Commerce, Bureau of Export Administration and the National Security Agency, Interagency Working Group on Encryption and Telecommunications Policy, A Study of the International Market for Computer Software with Encryption, June 1995.

³ US Chamber of Commerce, Telecommunications Task Force Report, 1995.

⁴ Economic Strategy Institute, Finding the Key: Reconciling National and Economic Security Interests in Cryptography Policy, Washington, D.C. March 1998. Analysis based on US Department of Commerce, US Industry and Trade Outlook, 1998,

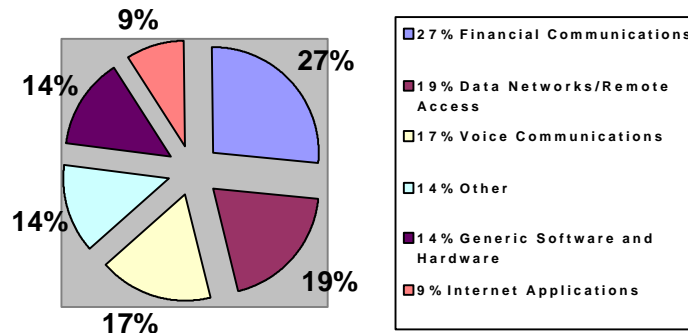
⁵ Ibid.

⁶ Ibid. Analysis from US Department of Labor, Federal Communications Commission, and the US Department of Commerce.

⁷ Ibid.

⁸ Economic Strategy Institute. From US Industry Outlook 1998.

Figure 2: Encryption Product Revenue by Application Type



Source: Economic Strategy Institute

Current US Regulations

Since encryption technology has traditionally been used by military and intelligence agencies, the US government classified advanced encryption as a munition, to be controlled under the International Traffic in Arms Regulations (ITAR).⁹ As a result, exportation and development of encryption products was closely scrutinized by the Department of State, which held supervisory authority over ITAR.¹⁰ After a review at the direction of President Clinton in 1993, domestic restrictions were relaxed, although export controls remained. In February 1996, an amendment to ITAR was passed, removing civilian encryption from the munitions list, creating an exemption for the temporary export of certain cryptography products.¹¹

On November 15, 1996, all previous restrictions concerning the exportation of mass-market encryption products were suspended by an executive order signed by President Clinton.¹² The order, which will expire on December 30, 1998, separates encryption products into three categories. They are products that incorporate key recovery mechanisms, products for which a key recovery mechanism is being developed, and products for which there are no plans to incorporate key recovery mechanisms in the future.

The executive order radically loosened the previous restrictions, which banned exportation of any products stronger than 40-bit. The new regulations continued the lack of restrictions on domestic use or import of encryption products. The new regulations also removed commercial encryption from the Munitions List, which transferred licensing from the State Department to the Commerce Department, with the Department of Justice having an advisory role in export decisions. Encryption products are now subject to the Commerce Control List and the Export Administration Regulations of the Commerce Department and its Bureau of Export Administration

⁹ United States Munitions List, International Traffic in Arms Regulations Category XIII (b)(1).

¹⁰ State Department authority is derived by the Arms Export Control Act (22 U.S.C. 2778).

¹¹ Department of State, Bureau of Political Military Affairs, Amendment to the International Traffic in Arms Regulations, 22 CFR, Parts 123 and 126 [Public Notice 2294].

¹² Memorandum and Executive Order 13026, November 15, 1996.

(BXA). Exports are subject to a case-by-case review to ensure that items do not violate US foreign policy and national security objectives.¹³

For non-key 40-bit encryption products, there is a license review process by the BXA.¹⁴ For products with key-recovery mechanisms, exporters are required to identify key-recovery agents and security policies for safeguarding the key and other decryption materials. For 56-bit products that do not already incorporate key-recovery mechanisms, exporters must provide a timetable that explains in detail the steps to be taken to develop such mechanisms within a two-year time frame. After this one time review, the producer can export up to 2 years, with the license granted in 6 month intervals to assure that the producers are making adequate progress in developing a key recovery mechanism. For products which do not incorporate key recovery mechanisms, the previous limit of 40 bits remains.

In May 1997, the Department of Commerce outlined another modification of export controls, allowing the exportation of non-key products of greater than 56-bit for use by financial institutions.¹⁵ These encryption products can now be exported if they are designed specifically for financial institutions, although exporters are still required to assist in the development of a key-management infrastructure. On July 7, 1998, the Administration announced plans to relax export controls for strong encryption software without requiring provisions for key recovery, but only for financial institutions in the 45 countries that have acceptable money laundering laws.

In the period from December 30, 1996 to September 26, 1997, 934 of 1,216 encryption products have been granted export licenses by the Commerce Department. The total value of the licenses awarded has been estimated at approximately \$3.3 billion.¹⁶ Although a number of US firms have already received export licenses for their encryption products stronger than 56-bit, these products have only been exportable to select customers, such as foreign offices of US businesses and international financial institutions. In general, mass-market software with powerful encryption has not been exportable under current law.

Most Recent Domestic Developments

On April 24, 1998 at a meeting of the Congressional Internet Caucus, Undersecretary of Commerce William Reinsch said that the government is working with industry to develop a plan on how to proceed after the executive order expires. Mr. Reinsch has most recently commented that the Administration was not currently looking for a legislative solution to the encryption issue. However, the Commerce Department and the Administration both realize the need to determine who will hold the keys and how law enforcement agencies will gain access to those keys.

¹³ White House Office of the Press Secretary, Memorandum on Encryption Export Policy, November 15, 1996, p. 2.

¹⁴ Federal Register Vol. 61, No. 251, pp. 68573-68587.

¹⁵ Bureau of Export Administration Press Release, Encryption Exports Approved for Electronic Commerce, May 8, 1997.

¹⁶ Commerce Department/Bureau of Export Administration estimate.

Law enforcement and intelligence agencies argue that it is necessary for their respective agencies to easily and secretly gain access to encrypted information. It is known that these agencies wish to create a third party key escrow system where they could gain easy access to keys without the users being aware. Comments by the FBI director Louis Freeh have made it clear that the FBI will advocate domestic controls of strong encryption, in addition to the export restrictions.¹⁷

Producers and consumers of strong encryption products oppose all restrictions, or at least want increasingly higher limits on the bit length, without regard to whether the product includes key recovery features. They argue that business should have access to the best encryption products available to ensure that competitors or other unauthorized parties cannot gain access to sensitive information. They also claim that restrictions reduce the willingness of consumers to buy products and services electronically, slowing the growth of electronic commerce.

Business has allied with numerous privacy and civil liberties organizations. Both want consumers to have the best products possible to protect personal, medical, and financial information. They note that strong non-key recovery encryption is already available worldwide, validating the idea that the US has already lost its ability to influence the availability of encryption worldwide.

The National Security Threat

Needs for Access to Encrypted Data

Supporters of encryption export controls insist that the law enforcement and national security concerns demand that the government be able to intercept and decrypt electronic communications when unlawful activities are suspected. They claim that the only method by which law enforcement agencies can easily and clandestinely gain access to the plain text information is by getting the key from a third party key escrow agent. They argue that this is the only means by which they can effectively investigate suspected encrypted criminal communications, and point to threats of national security and public safety that would arise if criminals used encryption that the US government agencies could not decrypt.

They state that the National Security Agency (NSA), has been able to thwart criminals and terrorists because they intercepted and decrypted communications in time.¹⁸ If those communications had been encrypted with strong encryption, their task would have been much more difficult or impossible. It should be noted that many of the cases where the NSA has intercepted electronic communications have remained classified, and cannot be used as examples in public debate.

¹⁷ Statements of Louis J. Freeh, director, Federal Bureau of Investigation, Committee on Commerce, Science, and Transportation, US Senate: "Impact of Encryption on Law Enforcement and Public Safety," p.1 July 25, 1996 <<http://www.fbi.gov/congress/encrypt/encrypt.htm>>.

¹⁸ Statements of Louis J. Freeh, Committee on Commerce, Science, and Transportation, US Senate, July 25, 1996.

Policy Objectives

The law enforcement and intelligence communities want all encryption products, both foreign and domestic, to contain key recovery features. In the best case scenario, the entire key would be held in escrow by a government agency. The key could then be obtained by a court order when criminal activities were suspected, in the same manner as current wire tapping laws. It is a long-term goal of the NSA to expand a domestic key management infrastructure into a global infrastructure.

Currently, the enforcement agencies know that it is unlikely that all of their demands will be met, especially concerning domestic controls and the government as the only designated key escrow organization. When the executive order became the new standard regulating proliferation of encryption products, it was hoped that the export controls would limit the availability of non-key products domestically, since companies are usually unwilling to develop two separate products for domestic and foreign sale. The export controls also influence which products are purchased domestically, since most of the users are multinational companies that plan to use the products in both domestic and foreign offices.

In 1993, the Clinton Administration proposed a voluntary use of key recovery agents, with NIST and the Department of Treasury jointly serving as key escrow agents. The industry strongly objected to the key escrow provisions, particularly to the fact that government agencies would hold the keys. Since this time, proponents of encryption restrictions have proposed that the keys be held by “trusted third parties.” The law enforcement community ideally wants a government agency to hold at least part of the key. To this end, it has been suggested that a new department be created to serve as a key escrow agent. This new department would also have control of which private organizations could be licensed to hold the other half of the key.

Economic Competitiveness and Privacy

Damage to US Development of Information Technology

US businesses and privacy groups argue that restrictions on sale of encryption products hinder development and economic growth. They point to the increased costs of developing two separate products for foreign and domestic sale. They also claim that the international demand for encryption products continues to increase while the US loses ground to foreign companies that can export their products regardless of strength or key recovery features.

US businesses claim that the National Security Agency overstates the usefulness of intercepting encrypted messages. Business and has tried to show that wire tapping is no substitute for other proven methods of gathering evidence that are much more effective. Businesses also worry about the security of key recovery products, and points to numerous studies which conclude that these systems are

inherently more vulnerable due to easy “back door” access, especially when a third party holds the keys.¹⁹

Many businesses which make use of encryption to secure electronic communications note that the spread of electronic communications and commerce are very dependent on peoples’ perception of the security of the communication medium. They point to surveys which show the importance of the consumer perception of the security of communications.²⁰

Challenges in the Courts

In August 1997, US District Court Judge Marilyn Patel ruled that current encryption regulations violate the First Amendment.²¹ Dr. Bernstein, a mathematics professor, tried to post his encryption source code on the Internet, and had plans to write and lecture about the code. He was blocked by State and Commerce Department regulations, which required a license before he could share his work with the international community. Within days, Internet sites across the globe posted his “Snuffle” encryption software code, defying attempts by the government to limit its spread.

Bernstein vs. Department of State brought encryption controls to the attention of civil liberty groups. They now acknowledge that encryption and cryptographic technology are becoming increasingly vital tools for human rights activities, political dissidents, and whistle-blowers throughout the world to facilitate confidential communications free from intrusion.²² In their view, just as mathematics text or written music communicates to a specially trained group of readers, a computer program communicates to its own group of readers.²³ If seen in this regard, First Amendment implications of computer programs are no different from those of many other copyrightable texts. To support this view, they point to previous rulings stating that “language is a sophisticated and complex system of understood meanings and is by definition speech, and the regulation of any language is the regulation of speech.”

International civil liberty groups note that countries which have the most strict laws limiting encryption technology are usually the same that limit freedom of speech and abuse basic human rights. Their studies show that thousands of illegal wire taps, most are used to monitor the activities of people and organizations that are considered to be enemies of the state, are placed annually.²⁴ They wish to make the public aware

¹⁹ Center for Democracy and Technology, “The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption,” Ad hoc Group of Cryptographers and Computer Scientists, May 1997 <<http://www.cdt.org/crypto/risks98/>> .

²⁰ Louis Harris and Associates, Inc., “E-Commerce and Privacy: What Net Users Want,” April 27, 1998. <http://www.aba.com/abatoll/showme_rel.html?location=Comply_Privacy_ExecSummary.htm>.

²¹ Bernstein vs. US Dept. of State, No. C-95-0582, 1997 US Dist. LEXIS 13146 (N.D. Cal. Aug. 25, 1997)

²² Banisar, David, “A Primer on Electronic Surveillance for Human Rights Organizations,” International Privacy Bulletin 3, July 1993.

²³ Ibid.

²⁴ Global Internet Liberty Campaign, “Cryptography and Liberty: An International Survey of Encryption Policy,” 1997 <<http://www.gilc.org/crypto/crypto-survey.html>>, June 22, 1998.

that the US government also has a record of using resources to gather intelligence on persons who may have never committed a crime, but may be considered dangerous to the stability of the country.

Policy Objectives

The policy objectives for the privacy groups and the business interests are the same. They oppose all restrictions to the development and sale of encryption products, and want the market to determine what kinds of encryption products are produced. They want the policy makers to realize that without a level international playing field, the US can not be expected to compete in the global market. More importantly, they want the public to realize that future leadership in the field of information technology will depend on leadership in the field of information security, and the demand will be met by foreign products if current restrictions continue.

Assessment

Foreign Policy Considerations

The need for international guidelines have emerged from the explosive worldwide growth of information and communications networks. The US has attempted to create a global key management infrastructure (GKMI), and unsuccessfully lobbied the Organization for Economic Cooperation and Development (OECD) to adopt its GKMI plan.²⁵ The official OECD guidelines for cryptography policy were released on March 27, 1997, and allows individual countries to develop their own policies, realizing that strong encryption technology is necessary for secure networks.²⁶ They state that while law enforcement should have access to plain text when given permission from the proper authorities, the fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.

After the unsuccessful attempt to lobby OECD, the US began to pressure the European Union to establish key recovery requirements. Again, the US was unsuccessful.²⁷ The EU situation brought attention to the difficulties of harmonizing multiple legal systems and perceptions of national security. The EU released its guidelines in October 1997, encouraging that inter-EU controls on commercial encryption products be progressively dismantled, and also recognized that a study of

²⁵ "US fails in Global Proposal for Internet Eavesdropping," John Markoff, *The New York Times, CyberTimes*, March 27, 1997 <<http://www.nytimes.com/library/cyber/week/032797code.htm>>.

²⁶ Organization for Economic Cooperation and Development, Recommendations of the Council Concerning Guidelines for Cryptography Policy, March 27, 1997.

²⁷ Europeans Clash with US Over Encryption," Matthew Slater, *TechWire*, October 9, 1997 <<http://www.techweb.com/wire/news/1997/10/1009clash.html>>.

existing regulations within the EU member states needed to be undertaken, with the goal of harmonizing the multiple control options.²⁸

The most current and complete international survey of encryption policy, undertaken by the Electronic Privacy Information Center (EPIC), on behalf of the Global Internet Liberty Campaign (GILC), shows that most countries do not have any restrictions to the sale of commercial encryption products.²⁹ The countries with the strongest restrictions on the sale of encryption products, notably China, Israel, Pakistan, Russia, and Singapore, are also those in which state security agencies play a dominant role in policy. Noting previous attempts by the US, it is clear that the international community is unwilling to implement the global key escrow system that the US endorses, and increasingly resents US pressure on what they consider a domestic issue.

Effectiveness of Current Policy on National Security

The primary national security threat posed by encryption technology is that it hinders the government's ability to gather intelligence. Widespread use of strong encryption technology may prevent the government from carrying out its previously less restrained monitoring of illegal activities. Increasingly, wiretaps are being frustrated by encrypted communications. Taking advantage of this, strong encryption technology will inevitably be used to aid terrorists, drug cartels, child pornographers, and other criminals to secure communications.

The US National Security Agency (NSA) worries about the effect that the proliferation of strong encryption will have on its signals intelligence (SIGINT) systems division. It is clear that proliferation will obstruct interception and monitoring of foreign and domestic communications.³⁰ Information gained by SIGINT is credited with avoiding casualties, preserving the peace, and helping to win wars. The NSA regards the continued operations of SIGINT to be of vital importance in the maintenance of US national security.³¹

It has, however, been shown that other methods of law enforcement have been effective in solving the majority of cases where encryption has blocked the collection of evidence.³² It is also expected that Law Enforcement will become more sophisticated in alternative methods of gathering data. It has been shown that in most of the cases where law enforcement has been hindered by encryption, authorities were able to gain access to the encrypted messages by cracking weak encryption or by obtaining the decryption key by consent, guessing, or by finding the physical medium

²⁸Office of Press and Public Affairs, European Commission Delegation, "European Commission Adopts Policy Framework for more Security on the Internet," press release, October 8, 1997 No. 66/97.

²⁹ Global Internet Liberty Campaign, *Cryptography and Liberty: An International Survey of Encryption Policy*.

³⁰ Center for National Security Policy, *Breaking the Code on the Encryption Debate: national Security Interests Are being Jeopardized*.

³¹ Center for National Security Policy, "Legislation Governing Encryption Must Protect American national Security Interests," n.d. <<http://www.security-policy.org/papers/97-D131.htm>>.

³² Dorhey E. Denning and William E. Baugh, Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information, September 3, 1997.

where the key is held. It should also be noted that in cases where encryption was unbreakable, other methods of gathering evidence were sufficient to achieve convictions.³³ This shows that in the majority of cases, encryption was not a barrier to successful law enforcement.

Effect of Current Policy on Civil Liberties and Privacy

It is very hard to assess the scope and the effects of unlawful monitoring of citizens, and the impact is hard to quantify. In many countries of the world, human rights organizations, journalists, and political dissidents are the most common targets of surveillance by government intelligence, law enforcement agencies, and other non-governmental groups.³⁴ The US Department of State, in its 1996 Country Reports on Human Rights Practices, reported widespread illegal or uncontrolled use of wiretaps by both government and private organizations in over 90 countries. In some countries, the state-owned telecommunications companies were active participants in helping to monitor human rights advocates.

The study notes that this is also a big problem in developed countries. A French special commission has estimated that some 100,000 illegal wire taps were conducted annually in France alone. There have been numerous cases in the UK which show that the British intelligence services routinely monitor social activists, labor unions, and civil liberties organizations. The European Parliament issued a report in January 1998, revealing that the US NSA was conducting massive monitoring of European communications.

Attempts by the US to push for the implementation of restrictive national and international laws regarding the use of encryption technology has been raised as a political and civil rights issue by sympathetic political parties and organizations. The control of encryption technology concerns human rights and matters of personal liberty, which affect individuals around the world. Human Rights groups note that the privacy of communication is explicitly protected by the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and also stress that freedom of speech is one of the US' most cherished values.

Effect of Current Policy on Business

Studies show that as foreign producers continue to create encryption products as powerful as those available domestically, export controls are having an increasingly negative effect on the US economy. The estimated costs to the US economy differ in reports by the National Security Agency, the Department of Commerce, and the Industry itself. The economic impact to US Businesses occurs in five major areas. They are:

- 1) Lost encryption product sales

³³ Ibid.

³⁴ Human Rights watch, Encryption in the Service of Human Rights, n.d. <<http://www.aaas.org/SPP/DSPP/CSTC/briefings/crypto/dinah.htm>>.

- 2) Slower growth in encryption-dependent industries
- 3) Forgone cost savings and efficiency gains from Internets
- 4) Indirect effects of current administration policy
- 5) Increased incidence of security breaches

It should be expected that in the absence of export controls, US producers should be dominating the global market. Instead, it is estimated that if current policies continue, the US encryption firms will lose between \$1.956 and \$9.288 billion in 1997-2002.³⁵

Software that requires incorporating encryption will also lose ground to competing products that offer higher levels of security. This includes the networking equipment industry, which supplies end-to-end products that make use of encryption technology. High-speed Internet connections, private label Internet Service Providers (ISPs), and web hosting, which are increasingly being offered and managed by US based Internet and Online Service Providers (OSPs), are facing problems in foreign markets due to their inability to export strong encryption. Many cellular, paging and wireless local-loop systems will have the ability to process financial transactions, and will require strong encryption that cannot be lawfully exported. Total losses in these areas are expected to total between \$12.107 and \$18.027 billion.³⁶

The public perception of the security of electronic communications markedly affects consumer confidence in electronic commerce. As a result, electronic commerce will lose revenue due to fewer online sales and higher online shopping costs. Without the ability of manufactures, wholesalers and retailers to guarantee secure inter-business networks with their suppliers abroad, security concerns will delay the introduction of new systems. Total cost to businesses was estimated between \$6.88 and \$19.09 billion.³⁷

Each of the above estimated impacts has implications for the entire economy. Less activity in these sectors creates slower growth throughout the entire economy. The cost of these indirect impacts have been estimated at between \$17.56 and \$45 billion in the period of 1997-2002. The total of these combined costs has been estimated at 37.5 to 96.93 billion from 1997-2002. This estimate increases rapidly if extrapolated past 2002.

The cost of increased security breaches due to the lack of strong encryption could greatly increase the above mentioned costs. It is difficult to estimate the frequency or the damages of such attacks, due to the fact that it is in the best interests of businesses and organizations to hide such attacks to support consumer and investor confidence. A survey conducted by the FBI and the Computer Security Institute found that 47% of sampled organizations had been attacked via the Internet in 1996, a 10% increase from the previous year.³⁸ It has been estimated that worldwide losses from

³⁵ All figures in the economic impact section of this report are taken from the Economic Strategy Institute report and are projected losses in the five year period from 1997-2005.

³⁶ Ibid.

³⁷ Ibid.

³⁸ Denning and Baugh. "Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism."

malicious hacking incidents are up 75%, with losses projected to be between \$40 and \$80 billion by the year 2000.³⁹

The latest threats to national security due to weak encryption are electronic terrorism and information warfare, whereby hackers can gain the capability to destroy and disrupt critical infrastructures, and to retrieve, alter, and retransmit classified and sensitive information. These crimes can be committed from any point on earth, with little means of discovering the source. The President's Commission on Critical Infrastructure Protection was created in July 1996 as America's initial effort to examine the potential weaknesses of information infrastructures.⁴⁰ It warns that the increase of computing power and interconnectivity of various networks and infrastructures makes it possible for "cyberterrorists" to attack, disable, and destroy major components of US infrastructure. These include telecommunications, power systems, banking and finance, transportation, utilities, government services, and emergency services. The commission identified industrial espionage, terrorism, information warfare, and criminal activity as activities that threaten US national infrastructures. The report acknowledges that the use of strong encryption is vital to securing critical infrastructure.

Policy Options and Recommendations

Export Control Options

It has been shown that the US has already lost its ability to influence the worldwide proliferation of non-key-recovery encryption products greater than 56-bit, due to unrestricted foreign competition. The result is that current export restrictions cost the US economy billions every year and has little or no effect on national security. Current restrictions will continue to harm US leadership in the information technology industry, and compromise economic and personal security and privacy.

In addition to the toll taken on US business interests, the international community will continue to be angered by US attempts to force a global key management infrastructure (KMI). Continued attempts by the US to push a global KMI will only increase opposition by civil liberty, humanitarian, and privacy groups, and will highlight the many current abuses of US intelligence operations. The US cannot expect to stop the proliferation of strong encryption technology without the support of the international community.

Recommendations on Pending Legislation

³⁹ William F. Hagerty, "The Growing need for Cryptography: The Impact of Export Control Policy on US Competitiveness," The Management Advisory Group, Computer Systems Policy Project, Dec. 1995.

⁴⁰ President's Commission on Critical Infrastructure Protection, Critical Foundations, n.d. <<http://www.pccip.gov/backgrd.html>>.

The SAFE Act and the E-Privacy Act are the only pieces of pending legislation that have been endorsed by business organizations. To be supported by business organizations a bill must:

- 1) Codify domestic use policy.
- 2) Prohibit mandatory use of key recovery mechanisms.
- 3) Give the Secretary of Commerce exclusive jurisdiction over export of commercial encryption.
- 4) Prohibit licensing of encryption products prior to export.

It would also be productive to business to include provisions that would:

- 1) Prohibit unauthorized transfer of keys.
- 2) Outline the procedure to gain access to encrypted data, including foreign communications.
- 3) Allow for the export of generally available encryption.

Civil liberty groups object to the provisions that make use of encryption in unlawful communications a crime, and business doesn't like bills have provisions that would restrict products that are not "generally available". They claim that this could make US manufacturers followers rather than leaders in developing new encryption products.

The SAFE Act is the first comprehensive encryption legislation to reach markup, and it is clear that each committee wishes to impose its interests into the legislation. The Justice, International Relations, and Commerce amendments would be acceptable to business organizations however, if the Rules Committee decides to incorporate the National Security and Intelligence amendments into the bill, industry and business organizations will drop all support for its passage.

For legislation to be acceptable to law enforcement, it will need to include provisions that would:

- 1) Criminalize the use of encryption in the furtherance of a crime
- 2) Create a "NET" center to keep up with emerging technologies
- 3) Require exporters of encryption products to notify the Department of Commerce on the products' encryption capabilities.
- 4) Conduct further studies that would analyze the affect of policy on national security and economics.

APPENDIX

Pending Legislation⁴¹

Three bills in the House and four in the Senate concerning encryption or related issues have been introduced in the 105th Congress. H.R. 1903 has passed the House. Hearings have been held by six House committees (Commerce, International Relations, Intelligence, Judiciary, National Security, and Science) and two Senate committees (Judiciary and Commerce, Science, and Transportation).

H.R. 695: Security and Freedom Through Encryption (SAFE)

On February 12, 1997, Representative Goodlatte introduced H.R. 695. It was referred to the Committees on Judiciary, International Relations, Commerce, National Security, and Intelligence. All five committees have completed markup, and some of the amendments have significantly changed the character of the original bill. Next, the bill will go to the Rules Committee to determine which, if any, of the versions will be the vehicle for further action. As introduced February 12, the bill will:

- 1) Codify existing domestic use policy.
- 2) Prohibit the mandatory use of key recovery.
- 3) Prohibit requiring anyone in lawful possession of a key to turn that key over to another person except for law enforcement personnel acting under law.
- 4) Makes it a crime to use encryption in furtherance of crime.
- 5) Gives the Secretary of Commerce exclusive jurisdiction over export of commercial encryption.
- 6) Prohibits export controls on “generally available” commercial encryption except for military end-uses or identified individuals or organizations in specific foreign countries.

As reported from House Judiciary May 22 (H. Rept. 105-108 Pt. I):

- Exempt members of the intelligence community (as well as law enforcement) from the prohibition against getting encryption keys if acting under law (Provision 3).
- Clarify that the new crime of using encryption in the commission of a crime applies only to the use of encryption to avoid detection of some other federal felony and only when it is knowingly and willfully used to avoid detection (Provision 4).
- Add a fourth section that directs the attorney general to collect data on cases in which encryption has interfered with, impeded, or obstructed the ability of the Justice Department to enforce law.

As reported from House International Relations July 25 (H. Rept. 105-108 Pt. II):

- Removes distinction between mass market and customized software (Provision 6)
- Expands provision 6 to include consumer products that do not necessarily fall under the umbrella of “computing products” and broadens the scope

⁴¹ Smith, Marcia S., “Encryption Technology: Congressional Issues,” Congressional Research Service Issue Brief, May 14, 1998.

and definition of “generally available” to include hardware with encryption capabilities.

- Adds a section regarding international cooperation.

Note: another amendment was defeated 13-22 that would have allowed the President to deny export licenses for national security reasons.

As reported from House National Security September 12 (H. Rept. 105-108 Pt. III):

- Replaced provision 5 with a new section that gives the Secretary of Commerce, with the concurrence of the Secretary of Defense, responsibility for the export of encryption not controlled through the Munitions List (military application encryption).
- Provides that encryption products may be exported following a one-time review if they do not exceed the level specified by the President as not harmful to national security, and directs the President to notify Congress within 30 days of enactment and annually thereafter on the maximum level of encryption that can be exported without harming national security.

As reported from House Intelligence September 16 (H. Rept. 105-108 Pt. IV):

- Requires exports of encryption products to submit to a one-time review and include features allowing for immediate access to plain text or to decryption information.
- Requires encryption products manufactured and distributed for sale or use in, or imported for sale or use into, the US after January 31, 2000 to include features that provide immediate access to plain text data or decryption information from the encryption provider; allows for use of encryption products currently employed even after January 31, 2000
- Allows for law enforcement access with delayed notification requirements similar to those allowed in current wiretap statutory provisions
- Provides civil remedies and criminal penalties for unlawful access to or disclosure of plain text or decryption information
- Requires US government procurement of encryption technology that includes features allowing for immediate access to plain text or decryption information. This amendment does not change law enforcement’s statutory requirements prior to interception oral, wire, or electronic communications, or stored data (law enforcement must have separate court order to have the data, including communications, decrypted).

As reported from House Commerce September 29 (H. Rept. 105-108 Pt. V):

- Modifies provision 5 by adding creation of National Electronics Technologies Center in the Department of Justice to help law enforcement keep pace with encryption technology
- Prohibits conditioning laws or regulations governing issuance of certificate of authentication or authority on a requirement to escrow or otherwise share private keys or conditioning licensing, labeling, or other regulatory scheme for any encryption product on a requirement for key escrow
- Requires an NTIA study on the implications of mandatory key recovery
- Increases penalties and modifies language concerning use of encryption in furtherance of a crime

- provides liability protection for those providing plain text to law enforcement or government entities pursuant to judicial process
- Note: An amendment was defeated 16-35 that would have, inter alia, imposed domestic restrictions.

S. 376: Encrypted Communications Privacy Act (ECPA)

On February 27, 1997, Senator Leahy introduced S. 376. The Senate Judiciary Committee held a hearing on key recovery on July 9, 1997. As introduced February 27, the bill will:

- 1) Prohibit mandatory use of key recovery but allow law enforcement to access the key under court order if key recovery is used.
- 2) Codify existing domestic use policy.
- 3) Give the Secretary of Commerce exclusive jurisdiction over commercial encryption exports.
- 4) Liberalize export controls.
- 5) Make it a crime to use encryption to obstruct justice.
- 6) Establish liability protection and penalties for “key holders”.
- 7) Established procedures for foreign governments to access keys or decryption assistance.

S. 377: Promotion of Commerce On-Line in the Digital Era (PRO-CODE)

On February 27, 1997, Senator Burns introduced S. 377. The Senate Commerce, Science and Transportation Committee held a hearing on the Burns bill on March 19. Senator Burns offered a version of S. 377 as an amendment to S. 909 during a markup of the latter bill, but the amendment failed 8-12. As introduced on February 27, the bill will:

- 1) Prohibit mandatory key recovery
- 2) Establish an Information Security Board as a forum to foster communication and coordination between industry and government.
- 3) Codify existing domestic use policy.
- 4) Give the Secretary of Commerce exclusive jurisdiction over commercial encryption exports.
- 5) Require 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 products encryption capabilities. This report would include the same information required under current regulations, but would be provided after export instead of as a condition of obtaining a license.

S. 909: the Secure Public networks Act

On June 16, 1997, Senators McCain, Kerrey, and Hollings introduced S. 909. The bill was referred to the Senate Commerce, Science and Transportation Committee,

which ordered it reported, amended on June 19. However, the report has not been filed and no hearings were held. As introduced June 16 the bill will:

- 1) Codify existing domestic use policy.
- 2) Establish penalties for use of encryption in commission of a crime.
- 3) Encourage but not require use of key recovery.
- 4) Establish procedures for governmental approval of key recovery agents and certificate authorities.
- 5) Require key recovery agents, whether or not registered by the government, to disclose recovery information to lawfully authorized federal or state government entities.
- 6) Provide liability protection for key recovery agents acting pursuant to the Act.
- 7) Require that encryption products procured by the US government or purchased with federal funds for use in secure networks to be based on a “qualified system of key recovery”.
- 8) Permit export of 56-bit encryption products without key recovery if they meet certain conditions.
- 9) Directs the President to annually review that limit and increase it for products where similar products are widely available or report from other nations.
- 10) Permit export of any strength encryption product if it is based on a qualified key recovery system and meets certain other conditions.
- 11) Establish an Information Security Board to make recommendations to the President and Congress on a variety of issues.
- 12) Allow the President to waive provisions of the bill for national security of domestic safety and security reasons

During markup, several amendments were approved including a Kerry amendment establishing an Encryption Export Advisory Board (EEAB) with four government (CIA, FBI, NSA and the White House) and four industry representatives to make recommendations on whether export exemptions should be granted for non-key recovery products stronger than 56-bits.

On March 4, 1998, Senators McCain and Kerrey issued a press release announcing modifications to the bill:

- The EEAB would be composed of eight industry and four government representatives who would “approve levels of encryption for export based on worldwide availability or anticipatory availability”
- The President could still veto the Board’s decisions for national security reasons, with notification to Congress required
- US companies could export products with optional recovery features to approved end users.
- Use of key recovery remains optional in the US, but when it is used, the key could “only be obtained by the government by a court order subpoena”, as opposed to several other legal means in the original bill

- Dual registration of certificate authorities and key recovery agents was eliminated.

S. 2067: Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY) Act

On May 12, 1998, Senator Ashcroft introduced S. 2067. It was referred to the Senate judiciary Committee. Senator Ashcroft's Subcommittee on Constitution, Federalism, and Property Rights held a hearing on the issue on March 17, 1998, that primarily addressed the constitutionality of requiring the use of key recovery. As introduced May 12, the bill will

- 1) Prohibit mandatory key recovery and codify existing domestic use policy.
- 2) Prohibit federal or state agencies from linking the use of encryption for authentication or identification to the use of encryption for confidentiality purposes.
- 3) Require that the use of encryption products be voluntary and market-driven.
- 4) Authorizes government agencies to purchase encryption products, but such products that use key recovery must be interoperable with commercial encryption products.
- 5) Sets forth procedures for US and foreign law enforcement agencies to access decryption keys or assistance in decrypting electronic communications or stored data
- 6) Establishes a National Electronic Technologies Center (NET Center) to help law enforcement keep pace with encryption technology.
- 7) Make use of encryption to obstruct justice a crime
- 8) Give the Secretary of Commerce exclusive control over commercial encryption product exports
- 9) Allow export of generally available encryption products after a one-time review except for products designed or modified for military use.
- 10) Permit unrestricted export of customized encryption hardware and software products if a comparable product is or will be available within 18 months from foreign sources.
- 11) Establish an Encryption Export Advisory Board to determine whether comparable foreign products are commercially available.
- 12) Prohibit restrictions on encryption exports for non-confidentiality purposes.
- 13) Provide that nothing in the Act limits 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.
- 14) Provides that the contents of electronic records in networked electronic storage be treated in law as though the record had remained in the possession of the person who created the record and that government entities may only access the contents of the record under circumstances specified in the bill

- 15) Provides 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 a trace devices.

H.R. 1903: The Computer Security Enhancement Act of 1997

On June 17, representative Sensenbrenner introduced the Computer Security Enhancement Act, H.R. 1903. The house Science Committee's Technology Subcommittee held a hearing on June 19, and the bill was reported on September 3 (H. Rept. 105-243). The bill amends and updates the Computer Security Act of 1987, enhancing the role of the National Institute of Standards and Technology (NIST). As passed by the House on September 16, the bill will:

- 1) Require NIST to promote the use of commercial-off-the-shelf encryption products by civilian government agencies.
- 2) Clarify that NIST standards and guidelines are not intended as restrictions on the production or use of encryption by the private sector.
- 3) Provide funding for computer security fellowships at NIST.
- 4) Require the National Research Council to conduct a study of public key infrastructures.

A section that required NIST to develop standardized tests and procedures to evaluate the strength of foreign encryption products was removed before passage. The bill was referred to the Senate Commerce Committee, which held a computer security hearing on February 10, 1998.

H.R. 1964: Communications Privacy and Consumer Empowerment Act

On June 19, 1998 representative Markey introduced H.R. 1964. The bill covers a range of computer privacy and security issues, and was referred to the Commerce Committee. As introduced February 12, the bill will:

- 1) Codify existing domestic use policy.
- 2) Prohibit the government (federal or state) from conditioning the issuance of certificates of authentication or certificates of authentication or certificates authority upon use of key recovery systems.
- 3) Prohibit 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.
- 4) Require 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 for improving data security. Such technologies would include encryption.

Some Organizations Advocating Proliferation of Strong Encryption Technology

Alliance for Public Technology (www.apt.org/apt)
American Association for the Advancement of Science (AAAS) (www.aaas.org)
American Bankers Association (www.aba.com/aba)
American Civil Liberties Union (ACLU) (www.aclu.org)
American Electronics Association
Americans for Computer Privacy (ACP) (www.computerprivacy.org)
Amnesty International (www.amnesty.org)
Business Software Alliance (www.bsa.org)
Cato Institute (www.cato.org)
Center for Democracy and Technology (www.cdt.org)
Citizens for a Sound Economy (www.cse.org/cse)
CommerceNet Network Services Working Group
Computer and Communications Industry Association
Computer Professionals for Social Responsibility (CPSR) (www.cpsr.org/home.html)
Computer Systems Policy Project
Consortium of Electronics manufacturing Association
Digital Future Coalition (DFC) (www.dfc.org)
Economic Strategy Institute (ESI)
Electronic Frontier Foundation (EFF) (www.eff.org)
Electronic Messaging Association (www.ema.org)
Electronic Privacy Information Center (EPIC) (www.epic.org)
Electronics Industry Alliance
Free Congress Research and Education Foundation
Fund for Constitutional Government (www.epic.org/fcg)
Global Internet Liberty Campaign (GILC) (www.gilc.org)
Human Rights Watch (HRW)
Independence Institute (The Institute)
Information Industry Association (www.infoindustry.org)
Information Technology Association of America (www.itaa.org)
Information Technology Industry Council (www.itic.org)
Institute of Electrical and Electronic Engineers (IEEE) (www.ieee.org)
International Information System Security Certification Consortium (ISC2)
Internet Architecture Board (IAB)
Internet Education Foundation (IEF)
Internet Engineering Steering Group (IESG)
Internet Free Expression Alliance (IFEA)
Internet Mail Consortium (IMC)
Internet Privacy Coalition
Internet Society (ISOC)
Multimedia Telecommunications Association
National Association of Manufacturers (NAM) (www.nam.org)
National Computer Security Association
Online Banking Association (www.obanet.org)

Organization for Economic Cooperation and Development (OECD) (www.oecd.com).
 People for the American Way (www.pfaw.org)
 Privacy International (PI) (www.privacy.org/pi)
 Progress and Freedom Foundation (www.pff.org)
 Semiconductor Industry Association
 Society for Electronic Access (www.panix.com/sea)
 Software Publishers Association
 Telecommunications Industry Association
 US Public Policy Committee of the Association for Computing Machinery (USACM)

Some Organizations Opposing the Proliferation of Strong Encryption Technology

US Department of Justice
 Interagency Working Group on Cryptographic Policy (IWGCP)

The Intelligence Community

