Securing Information Technology Through Cryptography: An Analysis of United States Policy

Loren S. Southard†

Loren Southard is a second-year MPA student with a concentration in intergovernmental management, and a Walcott Fellow. Mr. Southard graduated cum laude in June 1995 from the University of California, Riverside, with a bachelor's degree in political science and history.

Introduction

As the world ponders the beginning of a new century, the manner in which people communicate and gather information is evolving rapidly. Perhaps the most important tool in communicating and informing is the Internet, which was created nearly 20 years ago by researchers and educators who sought to share information. The Internet has become the mainstream "information superhighway" in the current Information Age, as an estimated 20 million people worldwide have turned to the Net to share information, research a topic, look up an address, or even get a date. But all those who think that information posted on the Internet is confidential are in for a surprise.

New computer technology has spawned a digital revolution that has increased speed, efficiency, and savings for the communication and exchange of information.

Data posted on the Internet and stored in electronic databases—business records, electronic mail, and private files—is alarmingly insecure. Any reasonably competent hacker with the right tools can invade systems that are designed to be impenetrable. As a result, nervous Internet users are demanding greater protection for their information.

Currently, the greatest single tool to ensure data security in cyberspace is cryptography, defined as the translation of ordinary text into a series of symbols that is indecipherable without the correct code. Regrettably, current cryptography export policy is not adequate to meet the demands of Internet users. Additionally, like so many public policy debates in the computer industry, the use of export control of cryptography is not a subject of universal agreement. In fact, government officials and the computer industry are engaged in the kind of conflict over cryptography policy that very well inhibits, instead of develops, the growth and strength of information protection.

With the ever-increasing use of electronic communications and data storage, the time has come to design a public policy for the use of cryptography that adequately balances all the interests involved in the debate, including law enforcement, national security, global economic competitiveness, and individual privacy.

Background: The Need to Secure Information Technology

Electronic data storage and on-line communications have grown exponentially over the past decade. New computer technology has spawned a digital revolution that has increased speed, efficiency, and savings for the communication and exchange of information. As a result, a wide variety of people are taking advantage of the new technology. Businesses use digital channels of communication for the exchange of sensitive information such as project proposals, corporate marketing strategies, research and development, bidding information, and even trade secrets. People may also use on-line communication to send letters and

conduct financial transactions. Sensitive data such as medical records, driving records, and credit histories are stored in computer databases.

Government agencies are beginning to rely upon the new technologies as well. The National Research Council's Committee to Study National Cryptography Policy pointed out the challenges of a developing global communication structure: "Increasing reliance on electronic commerce and the use of networked communication for all manner of activities suggest that more information about more people will be stored in network-accessible systems and will be communicated more broadly and more often, thus raising questions about the security of that information."[1]

The expansive growth of information technology has turned out to be a double-edged sword: as technology becomes more sophisticated, the ability of thieves to break into computer networks and databases and improperly gain access to information keeps pace.

Inevitably, growth of information technology has attracted malicious mischief. The expansive growth of information technology has turned out to be a double-edged sword: as technology becomes more sophisticated, the ability of thieves to break into computer networks and databases and improperly gain access to information keeps pace. Vandals, hackers, organized crime, business competitors, and intelligence agencies of foreign governments have targeted business, government, and private communication for theft of records, trade secrets, passwords, and other critical information. However, this widespread threat of unauthorized access is unacknowledged by many. Americans seem to assume that their privacy is protected amidst the growth of computer and communications technology.

Despite this general lack of acknowledgment of the possibility of trouble, the vulnerability of computer networks has not gone unnoticed. The United States General Accounting Office (GAO), in a 1993 report to Congress, pointed out that "Increased use of computer and communications networks, computer literacy, and dependence on information technology heighten U.S. industry's risk of losing proprietary information to economic espionage."[2] When the GAO was called upon by Congress to investigate the nature of the problem of economic espionage via computers, it found that "there was a growing problem for U.S. companies at home and abroad."[3] The FBI surveyed 400 companies and institutions in March of 1996 and found that over 40 percent reported break-ins, with 30 percent of these break-ins involving the Internet, despite the fact that these companies had in place a fire wall, a computer equipped with software that is supposed to only let legitimate traffic pass through.[4] Financial losses from computer crime has reached nearly $10 billion a year.[5] The GAO was unable in its study to determine the full extent of the problem because companies were reluctant to disclose the full extent of their vulnerability, fearing loss of shareholder confidence and the difficulty in placing a value on the proprietary data that was lost.[6]

Private citizens should also be concerned about the vulnerability of information technology. As G.A. Keyworth and David Colton wrote:

> Americans take it for granted that when they send a package via first class mail its contents are protected. We do not worry that someone will open our envelopes and take our checking or credit card numbers, read our personal letters or steal our business ideas. Yet our privacy could be threatened as we move to a digital economy and more information is shared electronically.[7]

Michael Froomkin also commented upon the vulnerability of private electronic mail messages by pointing out, "the ease with which electronic mail messages can be intercepted by third parties means that communicating by public electronic mail systems, like the Internet, is becoming almost as insecure as talking in a crowded restaurant."[8]

Even Internet companies are warning their own customers of the danger. Netscape Communications, Inc., the company that developed the popular Internet browser Netscape Navigator, acknowledges the potential threat to data being sent along the Internet. Any time a user of the browser attempts to send information such as e-mail, the following warning appears: "Any information you submit is insecure and could be observed by a third party while in transmit. If you are submitting passwords, credit card

numbers or other information you would like to keep private, it would be safer to cancel the transmission."[9] Using Michael Froomkin's analogy of talking in the restaurant, not only is the restaurant crowded, but the patrons are increasingly interested in the conversation.

Cryptography

The most important tool in securing information technology and bringing about the security mechanisms of traditional paper-based communications media—envelopes and locked filing cabinets—is cryptography, which allows for a degree of protection for communications and information stored and transmitted by computers.[10] The Internet Architecture Board and the Internet Engineering Steering Group, the entities responsible for setting the standards for the Internet, note that "Cryptography is the most powerful tool that users can use to secure the Internet."[11] Prior to the recent growth in information technology, cryptography technology was only critical to the federal government which used cryptography to secure sensitive State Department, Defense Department, and intelligence agency information.

Encryption involves the conversion of clear text into an unreadable form. Cryptographic technology involves two processes. The first process is the *encryption* process. Data is encoded or "scrambled" using an algorithm (mathematical procedure) and a randomly selected variable associated with the mathematic formula known as the "key."[12] Only the person who holds the key can conduct the second process, *decryption*. With decryption, the key interacts with the algorithm which brings the scrambled text back into readable form. Only the intended recipient of the data transmission, or someone legally entitled to access stored database information, can unscramble the information and gain access to the information.

The key consists of a string of numbers which, when used with the original mathematic formula, allows the encrypted information to be read. Key length is measured in "bits" with bit lengths beginning at 40 bits, 56 bits, and 64 bits. An example of a key would be an Automatic Teller Machine (ATM) personal identification number. The longer the key (i.e., the more numbers involved), the stronger the security. Each number added to the key increases the number of possible combinations which, in turn, increase the computing time and power that would be needed to break the code and access the encoded information.

The most important tool in securing information technology and bringing about the security mechanisms of traditional paper-based communications media—envelopes and locked filing cabinets—is cryptography, which allows for a degree of protection for communications and information stored and transmitted by computers.[10]

The ability to break a code increases exponentially with the size of the key. For example, a 90-bit key would be a quadrillion times tougher to break than a 40-bit key.[13] Jim Bidzos of RSA Data Security points out that "If you were to attack a 41-bit key, it would take twice as long as a 40-bit key."[14] Bidzos further adds, "If all the keys of a 40- bit key fit in a teaspoon, it would take a container the size of the planet earth to hold a 128-bit key."[15] Keys that are 56 bits are considered at the edge of today's technology.

When data is encrypted, it is important that the program be secure for a long time. Ian Goldberg, a graduate computer science student at the University of California, Berkeley, claimed, "It [the key] is no good if today it can't be broken but two months from now it can."[16] A panel of cryptography experts pointed out that in order to ensure that there is "adequate protection against serious threats," a minimum of 75 bits is necessary for protection and 90 bits would be ideal for protection from hacking for the next 20 years.[17]

The issue of key length has featured significantly in the recent debate over cryptography policy. Goldberg responded to a challenge by RSA Data Security Inc. to break a 40-bit key and access encrypted information. Using a network of 100 workstations at the University of California, Berkeley, Goldberg was able to crack a 40-bit code in three and one-half hours. Goldberg was able to test over 100 billion keys an hour and used over 1 trillion possible keys to break the code.[18]

Correctly designed cryptography not only assures the confidentiality of documents, but also affords authentica-

tion capability through the use of "digital signatures." A digital signature is "a cryptographic-based assurance that a particular file or message was created or transmitted by a given person."[19] Cryptography also allows for the ability to authenticate the integrity of transmitted data and verification of the sender of the data, much as a handwritten signature verifies the authenticity of a paper transaction. Another benefit of digital signatures is that of non-repudiation, which provides evidence that an authentic transaction took place. For example, if a customer places an order through the Internet, the customer's digital signature would be absolute proof that the order was placed. The growth in communications applications such as electronic mail and electronic fund transfers rely upon the authentication and confidentiality of encryption technology.

Cryptography can provide the confidentiality that is necessary for preventing crimes in legitimate business and personal transactions, such as the unauthorized interception of private electronic mail and the unauthorized disclosure of medical data. However, this confidentiality can also be used for illegitimate purposes. The National Research Council points out that "Although strong, automatic encryption implemented as an integral part of data processing and communication provides confidentiality for 'good guys' against 'bad guys' (e.g., U.S. business protecting information against economic intelligence efforts of foreign nations), it unfortunately also protects 'bad guys' against 'good guys' (e.g., terrorists evading law enforcement agencies)."[20]

Cryptography can provide the confidentiality that is necessary for preventing crimes in legitimate business and personal transactions, such as the unauthorized interception of private electronic mail and the unauthorized disclosure of medical data.

Louis Freeh, director of the Federal Bureau of Investigations (FBI), expressed reservations regarding cryptography and its potential use in testimony before Congress. Freeh stated, "Powerful drug cartels as well as terrorist organizations are aware of the hiding and concealing power of strong encryption and are making headway to develop that technology to defeat counter-terrorism investigations."[21] The concerns about the inappropriate use of cryptography have led to a contentious debate between the software industry and civil libertarians on one side and the Clinton administration and law enforcement agencies on the other.

The advent of the computer revolution has created a growing market for cryptography technology. Cryptography had long been reserved for protecting the confidentiality of military and diplomatic documents, but the increased use of the Internet for commerce and communication has increased demand for cryptography by business interests and private citizens. This demand goes beyond the borders of the United States, moreover, with foreign entities entering the competitive market. Customers around the world are seeking the technology that will ensure that their Internet transactions are secure. Not surprisingly, the global demand for cryptography has precipitated a contentious debate in the United States over cryptography policy.

The Policy of Export Control

Since foreign interests and criminal elements could easily invade American networks and evade law enforcement if they possess the right code-breaking technology, the United States has prohibited the export of cryptography and related technical data out of fear that this technology will fall into the wrong hands.[22] By contrast, no controls are placed on the domestic use of cryptography. While export controls have existed for a number of years, the Clinton administration recently attempted to establish a comprehensive policy that balanced the need for communications privacy with the need for access to communications by law enforcement and national security agencies. A civilian agency, the National Institute of Standards and Technology (NIST), was originally charged with the development of information policy through the Computer Security Act of 1987,[23] although the actual development of the policy took place in consultation with the National Security Agency (NSA).[24]

The general authority to establish export control policy is based on two pieces of legislation: the Arms Export Control Act (AECA) of 1949 and the Export Administration Act (EAA). The AECA established the legislative grounds for the International Traffic in Arms Regulations (ITAR), which defines the United States Munitions List (USML).[25] Munitions (military-sensitive items) are placed under the supervision of the State Department's Office of Defense Trade Controls, which must approve the export of any item on the USML. The approval process of the Office of Defense Trade Controls is often viewed by vendors and foreign purchasers to be a difficult, time-consuming process.[26]

Export controls tend to drive major vendors to a "least common denominator" cryptographic solution that will pass export review as well as sell in the United States.[33]

The EAA provides the legislative basis for the Export Administration Regulations (EAR), which establish dual-use items (having both military and civilian applications) that are then placed on the Commerce Control List (CCL).[27] The CCL is administered by the Commerce Department and is reviewed only once by the U.S. government in order to simplify the marketing and sale of a product overseas.[28] Products on the Commerce Control List receive a more liberal export consideration than items on the United States Munitions List. The National Security Agency reviews encryption products and gives its opinion on whether the product should be placed on the more restrictive munitions list or the more liberal Commerce Control List.

Under the authority of the International Traffic in Arms Regulations, all "cryptographic systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems" are subject to review for placement on the munitions list.[29] However, certain exemptions related to bit length of the key were made for cryptography to be regulated as a dual-use item and placed on the Commerce Control List. Still, the software industry is only allowed to export items with 40-bit keys.[30]

Law enforcement and national security concerns have greatly influenced export control policy. Law enforcement agencies fear that their ability to conduct investigations will be hindered by widespread use of cryptography. In testimony before Congress on April 27, 1995, FBI Director Louis Freeh warned of "terrorists communicating over the Internet in encrypted conversations, for which we will have no available means to read and understand."[31] But critics of the export control policy claim that such danger is overstated. The Internet Architecture Board and the Internet Engineering Steering Group, in a joint statement released on July 24, 1996, claimed that "such policies [export controls] are against the interests of consumers and the business community, are largely irrelevant to issues of military security and provide only a marginal or illusory benefit to law enforcement agencies."[32]

Paradoxically, strict export controls have hindered the availability of effective security measures in this country. For example, the global nature of the Internet requires the "interoperability" of computer systems, that is a United States system has to be able to communicate with a European system. If these interoperative systems are using cryptography, both users must encrypt and authenticate information using the same cryptographic formula. However, if users of the European systems are unable to decrypt messages sent from American users because U.S. encryption technology is restricted in Europe, the interoperability of the global system is defeated. To remedy this problem, U.S. software companies produce products with relatively weak cryptography—key lengths of 40 bits and below—that will pass the export restriction. These products thereby lower the overall strength of cryptography in this country. Thus, export controls tend to drive major vendors to a "least common denominator" cryptographic solution that will pass export review as well as sell in the United States.[33]

The United States software industry, the worldwide leader in the development of computer programming, has bristled under the export controls. One concern is the potential loss of market shares overseas for United States companies. A recent report prepared by the Commerce Department and the National Security Agency entitled "A Study of the International Market for Computer Software With Encryption" pointed out that U.S. companies will

lose market share in the international cryptography market to foreign encryption products. The Computer Systems Policy Project has estimated that unless the export controls are lifted, "the U.S. technology industry will lose $60 billion in revenues and 200,000 jobs by the year 2000."[34] The GAO has also alluded to the weakness of the export control policy in noting that "a German company contracts with a Japanese company to manufacture a high-speed encryption chip for export to Germany. In contrast, U.S. export controls prevent U.S. companies from exporting such a chip to the German company."[35] Export controls also put U.S. companies that do business with foreign-based companies or have branches based outside the country at a disadvantage since U.S. companies are unable to securely and easily engage in electronic commerce.

A cryptography policy of export control is no longer politically viable in the United States. Five bills recently introduced in Congress testify to congressional realization of the limitations of the export control policy. The Promotion of Commerce On-Line in the Digital Era Act (Pro-Code), proposed by Senator Conrad Burns (R-MT), would have abolished controls on encryption and would have prohibited the federal government from both restricting the sale of encryption and attaching conditions to any sale.

Support for the policy of export control is practically nonexistent outside of the law enforcement advocates within the Clinton administration. A large number of constituent groups, ranging from software industry representatives to civil liberties groups, lobbied against the export control policy. As IBM points out, "For the first time, government, industry, consumer groups, civil liberties groups, and the media around the world appear to agree it is time to reform public policy on cryptography."[36] The Administration appeared to acknowledge these concerns on October 1, 1996, when the president proposed a plan to relax the export controls but with restrictions.

Developing a Balanced Approach to Evaluating Cryptography Policy

A major criticism that the National Research Council directs at the current policy is, "For many years, concern over foreign threats to national security has been the primary driver of a national cryptography policy."[37] Designing a new approach to United States cryptography policy must synthesize many interests, including law enforcement and national security concerns, global economic competitiveness, and individual privacy.

Information Security

Information security interests take into consideration whether or not a proposal maintains or increases the level of security available through on-line communications and data storage. Concerns over interoperability have created a "lowest common denominator" effect that has watered down the strength of cryptographic technology. But any new policy that results in decreased information security would be ineffective. Proposals in cryptography should therefore offer a step forward in advancing the strength of information security.

While current law does not place any formal restrictions on domestic use of products with encryption capabilities, this policy only applies to stand-alone, security-specific cryptography products. However, the largest market is for integrated products in which a primary program is integrated with encryption capabilities such as e-mail programs and Web browsers.

Designing a new approach to United States cryptography policy must synthesize many interests, including law enforcement and national security concerns, global economic competitiveness, and individual privacy.

The Netscape Navigator, the leading Web browser on the market, is such a product. The browser can be obtained in two ways: it can be downloaded over the Internet or bought in the store. Not surprisingly, downloading the Navigator is more convenient. What is not evident is that in order to market the browser over the Internet, the lowest possible encryption is loaded into the program. The shrink-wrapped version, on the other hand, includes the highest possible encryption. As a result, the strength of information security capabilities in the downloaded version—the most widely-used by the American public because of its convenience—is in question.

For the past 25 years, the United States has led the way in developing computer and communications technology.

Global Economic Competitiveness

For the past 25 years, the United States has led the way in developing computer and communications technology. In fact, the U.S. digital industry is a $1.5 trillion industry.[38] The global growth in the use of information technologies has caused an increased demand for cryptography. But, as already mentioned, export controls of cryptography threaten the American leadership in computer technology.

Cryptography policy needs to elevate the economic competitiveness of the software industry. However, concerns of economic competitiveness extend beyond that of just the software industry. The economic opportunities of all U.S. companies operating in the global marketplace would be supported by the ability to use cryptography for their international business activities.

Privacy

Several civil liberties organizations, such as the Electronic Privacy Information Center and the Progress and Freedom Foundation, have voiced concerns about privacy in relation to controls on cryptography. The concerns of these groups focus on what they believe are infringements upon the constitutional protections of privacy.

The right to communications privacy has been upheld by the Supreme Court in several cases which have expanded the Fourth Amendment protections against unreasonable searches and seizures and the right to be secure in one's home and effects. In one such case, *Katz v. United States*, the Supreme Court held, "the government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied."[39] The case established guidelines whereby the government must use due process and obtain a warrant to conduct a wiretap.

In a brief of amici curiae filed in conjunction with a pending case, *Karn v. U.S. Department of State and Thomas E. McNamara*, lawyers representing the Electronic Privacy Information Center point to the possibility that "Cryptography may, in fact, provide the only effective defense against indiscriminate wiretapping in the emerging global network."[40]

Civil liberties advocates also point out that cryptography controls are unconstitutional since computer code is protected speech, a principle established in *Bernstein v. U.S. Department of State*.[41] Daniel Bernstein, a math professor at the University of Illinois, filed the suit in 1994 after the State Department told Bernstein that he could not publish an encryption program without registering as an arms dealer and acquiring an export license. U.S. District Court Judge Marilyn Patel ruled in favor of Bernstein in April 1996. Judge Patel held that software source code is protected speech, writing that "Like music and mathematical equations, computer language is just that—language—and it communicates information either to a computer or to those who can read it. For the purpose of First Amendment analysis, this court finds that source code is speech."[42] Judge Patel issued another ruling in December 1996 which declared that government export controls violated the First Amendment because these controls "create an atmosphere of 'prior restraint,' and thus restrict constitutionally protected speech."[43] The case is expected to be appealed.

The final chapter has not yet been written regarding the First and Fourth Amendment protection of cryptography. Judge Patel's ruling in the *Bernstein* case offers First Amendment protection to software source code but does not apply to real world software (such as e-mail programs and Web browsers) or "object code" that use encryption. Therefore, Netscape would still be unable to ship its Web browser with strong built-in encryption.

National security and law enforcement concerns are the impetus for the creation of cryptography policy.

Law Enforcement/National Security

National security and law enforcement concerns are the impetus for the creation of cryptography policy. Any proposal to change U.S. policy must allow communications and stored information of foreign entities hostile to the United States and criminal elements to be made

available to law enforcement and national security agencies as necessary.

The National Research Council voices another consideration regarding national security and the policy of export controls in pointing out, "export controls on products with encryption capabilities may well have a negative impact on U.S. national security interests by stimulating the growth of important foreign competitors over which the U.S. government had less influence and possibly by damaging U.S. competitive advantage in the use and development of information technology."[44] The United States is a leader in creating information technology standards throughout the world. By changing the current policy, the United States government would still have a major hand in how cryptography policy is developed on the international stage. If United States cryptography policy is not changed, on the other hand, the United States government could lose its global leadership in assuring the security of the Internet.

Political Viability

Any change in United States cryptography policy must meet the concerns of both the Clinton administration and the Republican-controlled Congress. The Clinton administration has been unwilling to stray from the concerns expressed by the National Security Agency, the primary goal of which seems to be keeping cryptographic code-breakers out of the hands of criminals and foreign terrorists.

Meanwhile, Congress has expressed considerable interest in this topic, as evidenced by the recent hearings held on the issue and the number of bills introduced. In the 105th Congress, Senator Conrad Burns (R-MT) introduced in the Senate the Promotion of Commerce On-line in the Digital Era Act or Pro-Code (S. 1726) which aims to overturn the Clinton administration export controls. In the House, Rep. Bob Goodlatte (R-Va) introduced the Security and Freedom through Encryption Act in the 104th Congress and has said that he will do so again in the 105th Congress. Both bills generated bipartisan support, but were unable to reach the floor of either the House or Senate. A growing number of Republicans in Congress fault Administration efforts to link export controls to key escrow proposals and criticizes the Administration for failing, "to recognize that top-down government-imposed policies are doomed to defeat."[45]

Approaches to Cryptography Policy: The Alternatives

While there are varied approaches toward United States cryptography policy reform, three major alternatives exist. The first alternative is the elimination of all export controls and complete free trade of encryption, which is strongly advocated by civil liberties groups and a group of advocates in the software industry. The second alternative is the new Clinton administration policy which went into effect on January 1, 1997, and which seeks to loosen export restrictions but ties this loosening to several conditions. The third alternative, which is advocated by such groups as the National Research Council and growing numbers in the software industry, proposes the relaxation—but not the complete elimination—of export controls through the use of a modified "key escrow" system.

Elimination of All Export Controls

The total elimination of export controls is supported by a diverse group that ranges from Internet advocates like the Internet Architecture Board and Internet Engineering Steering Group, to civil liberties organizations like the Electronic Privacy Information Center and the Center for Democracy and Technology. Advocates for this alternative gained congressional support when Senator Burns introduced his Pro-Code bill. Senator Burns' bill would have authorized the export of computer software with encryption for nonmilitary use to any country in which such software is permitted, unless "there is substantial evidence that such software will be diverted to a military end-use or an end-use supporting international terrorism."[46]

Eliminating export controls completely would likely have the effect of improving the level of security in digital communications. The "least common denominator" effect—whereby the U.S. software industry has created bare minimum cryptography for domestic use and that stays off the munitions list—is likely to disappear with the absence of controls. U.S. software companies would be able to concentrate on developing stronger cryptography, without having to worry about exceeding the weak 40-bit key length threshold. Since the strength of cryptography would certainly increase with the elimination of export controls, this policy would improve the level of security for computer transmitted information.

The economic competitiveness of the U.S. software industry is also likely to be strengthened by the elimination of export controls. As pointed out earlier, the industry could face a potential loss of $60 billion by the year 2000 if export controls are maintained.[47] More than 28 countries currently produce cryptographic software. Export controls cannot stop a foreign scientist from developing strong encryption products to fill the void created by the export control policy. The elimination of export controls would ensure that American leadership in information technology will continue, unencumbered by restrictions. U.S. businesses outside of the software industry that conduct worldwide transactions would also benefit as a result of increased confidence in the security of their business transactions, without concerns over weak cryptography or interoperability.

Key escrow has often been offered as a compromise solution to the strict export control policy.

Civil liberties advocates are strong supporters of the elimination of all export controls because this policy alternative would address their First and Fourth Amendment concerns relating to electronically stored information.

However, the policy of eliminating all controls fails to acknowledge the arguments made by law enforcement and national security agencies. Representatives from the FBI and the National Security Agency have repeatedly said that, "unregulated encryption will only increase the chance of international communication and the threat of terrorism."[48] Although law enforcement may be willing to endorse a softer line regarding export restrictions, their condition would be access to encrypted information that may be used illegally. Eliminating all controls clearly does not adequately address national security concerns.

Eliminating export controls also lacks political viability. Senator Burns' bill, which would have implemented this policy alternative, failed to pass through committee. Burns has recently introduced legislation that would eliminate exports controls in the 105th Congress. While there does appear to be a growing sentiment on Capitol Hill that cryptography policy should be changed, there are few signs that the changes would involve the complete elimination of export controls. The Clinton administration is unlikely to endorse this policy as well. Administration officials believe that the export liberalization bill goes too far.[49] While the Administration has backed away from its previous stance of strict controls, its latest proposal of relaxing restrictions does not indicate future elimination of all restrictions.

Key Escrow - Two Approaches

A major point of debate regarding U.S. cryptography policy is the proposed "key escrow" system. Key escrow has often been offered as a compromise solution to the strict export control policy and there are two major cryptographic policy alternatives that include a key escrow system.

Key escrow involves giving the encryption key to a neutral third party that stores the key. Should law enforcement agencies have reason to decrypt encrypted messages, the agencies would have to obtain a court order for the third party to release the key to give law enforcement access to the information. The concept of key escrow can be compared to a homeowner giving a trusted neighbor a copy of the keys to his home in case the homeowner is inadvertently locked out of his home. As with a third-party key escrow system, however, there are vulnerabilities within this scenario to which critics point as major drawbacks.

Drawing again upon the homeowner's scenario: While the neighbor may be trustworthy, other people, including members of the neighbor's family, may acquire access to the key which would be unacceptable to the homeowner. Through this kind of vulnerability, giving the key to a third party, the privacy of encrypted information is now exposed.

Law enforcement agencies strongly contend some type of back door is needed, whereby encrypted information can be accessed if necessary. But, organizations such as the Center for Democracy and Technology (CDT), a nonprofit organization that advocates new computer and communications technologies that advance constitutional civil liberties, claim that such a back door (key escrow) violates our right to privacy since it mandates giving the key to private information to a third party.[50]

The software industry appears to be leaning toward the kind of restriction maintained by a key escrow system.

Leaders of 11 major information technology vendors, including Apple Computer, IBM, and Digital Equipment Corporation, created an alliance to develop an exportable approach to cryptography.[51] The alliance's approach will not support complete elimination of restrictions but recognizes the need for national security measures as evidenced by the comments of Sam Fuller, vice president of Digital Equipment Corporation. Fuller states, "strong encryption is a necessary element in delivering secure network business solutions to our customers worldwide. Key recovery [escrow] is a mechanism that addresses government policy concerns about the export of strong encryption while at the same time meeting growing commercial needs."[52] Jim Bidzos, President of RSA Data Security added, "Export controls are a fact of life."[53]

Clinton Administration Proposal — Strict Key Escrow

The Clinton administration backed away from its previous policy of tight export controls in rules proposed in October 1996 and put into effect on January 1, 1997.[54] The Administration acknowledged the concerns expressed by the technology industry and sought to liberalize the policy of export controls on cryptography. In outlining the philosophy behind the Administration's new proposal, Vice President Al Gore stated, "President Clinton and I are committed to promoting the growth of electronic commerce and robust, secure communications worldwide while protecting the public safety and national security."[55]

According to preliminary rules released by the Commerce Department in December 1996, this policy would lift export restrictions on 56-bit key length encryption technology after a general, one-time licensing review was conducted to determine if the restriction on an encryption product could be lifted. Parties who apply for licensing under this program would be compelled to release their keys to escrow within two years. Within the two-year time frame, the exporter of cryptography must submit detailed business and marketing plans to the Commerce Department's Bureau of Export Administration every six months in order to have the export license renewed.[56]

The lifting of the restriction would also be contingent on an agreement to give the keys to a third party, hence a key escrow system. This key escrow proposal would establish a third party, selected by the government, that would store the keys and law enforcement officials, under the authority of a court order, could access the key to unlock encrypted documents.[57] However, domestic use of key escrow would be voluntary as the Administration keeps to the policy of not mandating the regulation of domestic cryptography.[58]

The software industry won further concessions when President Clinton, through Executive Order, moved cryptography off the State Department Munitions Control List and onto the "dual-use" Commerce Control List.[59] Moving cryptography to the discretion of the Commerce Department is a departure from the previous policy of tying cryptography to International Traffic in Arms Regulations. Nevertheless, this strict key escrow policy addresses the concerns of law enforcement and national security. While the export controls are loosened somewhat, law enforcement agencies are still allowed the minimum "backdoor" requirement whereby they would still have legal access to encrypted information.

Other concerns such as economic competitiveness need to be considered when allowing for the export of encryption technology. The overall policy which was put into effect by the Clinton administration, while straying from the stringent export controls, offers some "strings attached" policy in which licensing of trade is tied to the willingness of companies to comply with the Administration proposal.

At the same time, however, this form of cryptography policy is an improvement over the export control policy which watered down the strength of U.S. cryptography. However, the 56-bit limit still does not provide the strongest cryptography available. The Business Software Alliance (BSA), a trade group representing the software industry, had been lobbying for an adjustment to the 56-bit limit every two to three years to adjust to the increased sophistication of hacking techniques.[60] These concerns were not addressed in the new policy.

The success of this policy alternative in improving economic competitiveness depends upon the willingness of foreign companies to use key escrow cryptography. If non-key escrow cryptography is available to these companies, there is no reason to expect the companies to acquiesce to the demands of the United States government. Senator Patrick Leahy (D-Vt) points out, "Conditioning foreign sales of products with DES [56-bit keys] on development of key recovery systems puts enormous

pressure on our computer industry to move forward with key escrow whether their customers want it or not."[61] At this time, there is no evidence to show that foreign companies will accept the strict key escrow policy.

There are privacy concerns involved with this policy, particularly about upholding the constitutional protection of privacy and against unreasonable searches and seizures. The policy is troublesome because it makes information security contingent upon the fidelity of three actors— the sender, receiver and hey holder of encrypted information—while previous policy needed the trustworthiness of only two actors, the sender and the receiver. At issue is the government control of third party selection. As Jim Bidzos suggests, when the government shows up at someone's door armed with a search warrant, a citizen will let them in. There is no need to make up keys to your home and give them to the government in advance. He claims that this is essentially what the government is asking the software industry to do.[62]

More specifics are needed in order to ensure that questions regarding unlawful access of information by third parties is addressed. What is promising about the proposal is that should law enforcement need to decrypt encrypted information, law enforcement must first obtain a proper court order. Despite the assurances that proper due process will be followed by law enforcement in the access of keys, the ambiguity of the current policy over who controls the keys keeps this proposal controversial.

The software industry, while concluding that some form of key escrow is inevitable, has opposed the new policy. BSA has vowed to lobby against the new rules set forth by the Clinton Administration. Becca Gould, vice president for public policy at the BSA said, "We call it unworkable. We think these regulations should be thrown out in their entirety."[63] The BSA believes that key escrow should be market driven and voluntary and that there should be an unlimited key length allowed for key recovery products.[64]

Political viability of the new strict key escrow system is questionable. With the 105th Congress yet to address the issue, the popularity, or lack thereof, on Capitol Hill of this new proposal is ambiguous. However, Senators Patrick Leahy and Conrad Burns have come out in opposition to this new "strings attached" policy alternative. Senator Burns pointed out that the Administration policy "raises more questions than it answers."[65] Burns was troubled by the fact that Congress was not involved in developing the new policy—Clinton, using the power of Executive Order, went around Congress to establish the new policy—and said, "I can't say I'm pleased with a process that has all but excluded Congress and the public from the discussion."[66] Burns, who failed to pass his bill in the 104th Congress to do away with any export restrictions, has reintroduced such legislation in the 105th Congress.

The new Clinton administration policy is proposed to be in effect for two years, at which time it can be re-evaluated or changed. With two prominent senators, one from each side of the aisle, questioning the new Administration policy, the strict key escrow policy alternative stands on unstable ground. The Clinton administration's proposed changes to cryptography policy does not go far enough to address concerns over privacy and economic competitiveness. Perhaps most important, the Administration's insistence that the United States government control the key escrow system keeps this policy from becoming a viable option in reforming cryptography policy.

The Modified Key Escrow System — A Compromise Approach

In order to bring about a broader consensus on the cryptography policy problem, Congress, in the Defense Authorization Act for Fiscal Year 1994, called upon the National Research Council (NRC) to "conduct a comprehensive study of cryptographic technologies and national cryptographic policy," and to assess the "effect of cryptographic technologies on national security and law enforcement interests of the Unites States citizens; and the effect on commercial interests of the United States industry of export controls on cryptographic technologies."[67] The NRC gathered a well-rounded group of 20 experts in the field who concluded that U.S. policy should be changed and that "current national cryptographic policy is not adequate to support the information security requirements of an information society."[68]

In the report, *Cryptography's Role in Securing the Information Society*, the NRC put forward a comprehensive policy that balanced the national security and law enforcement needs with other concerns, mainly global economic competitiveness and privacy. Major recommendations included: (1) a policy that does not limit or regulate the use of domestic encryption; (2) making national policy more closely

aligned with market forces; (3) export controls should be relaxed but not eliminated; and (4) the new policy should assist law enforcement and national security in adjusting to the new technical age.[69] The NRC report provides a valuable groundwork for establishing a policy that can bring together the seemingly disparate concerns of national security, privacy, and economic competitiveness. However, the NRC does not endorse a key recovery system. To hasten a consensus, it may be time to put the key escrow system on the table as the best approach toward compromise, but the keys should be kept in control of the software companies until mandated to be released to the government by court order.

Security issues fare better under this modified key escrow policy than under the Clinton administration policy. The proposal calls for 56-bit key length cryptography to be easily exportable and available. Also, products that provide stronger protection would be made available to a list of approved companies, foreign subsidiaries, and approved foreign interests if these companies were willing to provide access to the encrypted information when legally called upon.[70]

Relaxing the export controls through a key-escrow system controlled by the software companies offers a balanced policy that weighs concerns about national security, economic competitiveness, and individual privacy.

Non-government use of cryptography is inevitable, and U.S. policy should facilitate this transition. The NRC points out, "National cryptography policy has become increasingly disconnected from market reality and the needs of parties in the private sector."[71] The proposed relaxation of the export control and the use of a list of approved companies who are allowed to import American cryptography will help establish the U.S. technology industry as an important actor in the trade of technology. Non-computer related industries, as well as their foreign subsidiaries and trading partners, will benefit from the strongest cryptography available, provided that they are on the approved list of commercial users. This is a positive result because, as Irving Wladawsky-Berger of IBM notes, "Once businesses are confident that their electronic transactions are safe...a flood of new market opportunities will open."[72] The relaxation of the export restriction and the creation of the approved commercial users list will aid in increasing the economic competitiveness of the U.S. software industry as well as other businesses which seek to use the Internet to conduct global business.

Civil liberties critics have problems with the modified key escrow proposal. These critics believe that this system would involve prior restraint and infringe upon Fourth Amendment protections. However, the basic right to privacy is not violated as law enforcement agencies will have to follow due process in order to gain access to keys to decrypt information. This policy differs from the new Administration proposal in that the keys would not be held by a third party, government entity. Instead, the keys would be held by the software companies who would release them upon court order. A unique proposal made in the NRC report is that the federal government begin to use key escrow encryption in order to calm the concerns of critics and to study, first hand, any difficulties that would arise from using a key escrow cryptography.[73]

Law enforcement concerns are effectively addressed by this policy, and they are synthesized with the concerns of businesses and individuals. A "backdoor" is still available through the modified key escrow approach. Also, the creation of a list of approved companies will compel these companies to follow the letter of the law in order to remain on the list. The NRC calls for Congress to consider legislation that would create criminal penalties if encrypted communications is used with the intent to commit a federal crime.[74] The modified key escrow approach is by far the best proposal put forward that balances law enforcement and business concerns.

Congress seems more receptive to this modified key escrow system. Senator Burns criticized the new Clinton proposal as incongruent with the NRC report, but the differences are not that dramatic.[75] Therefore, it appears that a compromise will need to be reached. The NRC report offers the greatest amount of common ground. Therefore, the proposals of the NRC report, while not immediately enacted by the Clinton administration, should be incorporated in a compromise with Congress as a politically viable alternative.

Based upon the analysis of these three leading proposals—elimination of all export controls, strict key escrow, and modified key escrow—the modified key escrow system is clearly the best alternative for reforming U.S. cryptography policy. Of all of the proposals, the modified key escrow approach best addresses the concern that export controls have weakened cryptography abroad and hindered the availability of strong encryption technology in this country as well. The current U.S. policy does not adequately balance all of the interests involved in the cryptography debate. In the modified key escrow proposal, however, all sides of the debate are considered. More importantly, this policy appears to be more amenable to the international community. Relaxing the export controls through a key-escrow system controlled by the software companies offers a balanced policy that weighs concerns about national security, economic competitiveness, and individual privacy.

It is necessary for some sort of consensus to be reached regarding U.S. cryptography policy so the United States can begin to clear a path toward a global policy on cryptography.

Need for Global Cooperation

It is necessary for some sort of consensus to be reached regarding U.S. cryptography policy so the United States can begin to clear a path toward a global policy on cryptography. The Internet is a global entity. Any United States policy must take into consideration international dimensions, among those being the possibility that, as the NRC points out, "the United States today does not have unquestioned dominance in the economic, financial, technological and political affairs of the world as it might have had at the end of World War II."[76] Consequently, the United States cannot simply dictate global cryptography policy because foreign competition is rising to the occasion and challenging the United States' edge in these technologies.

The concept of global interoperability is of the utmost importance if the global Internet is to operate smoothly. For the Internet to run smoothly, all nations must be operating under a system that ensures that information can be obtained and shared without disruption due to differences in hardware and software. Achieving global interoperability presents a difficult challenge. International governments are concerned with many of the same issues that have framed United States cryptography policy: national sovereignty, national security, and economic competitiveness. Therefore, it is important for any cryptography approach that includes key escrow to allow software companies to keep control of the keys, not a third party selected by the U.S. government or the U.S. government itself. U.S. policymakers must begin negotiations with foreign nations if they want to establish a global cryptography framework that has a key escrow system as its basis. IBM has noted:

> Experience demonstrates that such controls work only when governments of countries that serve as the principal sources of these products and technologies all agree on the means by which to affect these controls. The nature of technology — particularly in a global and fast-moving technology like electronics — is such that governments' control systems are inevitably challenged by the portability of technology and the speed of its development. Thus, agreements among supplier countries must be sufficiently adaptable to changing circumstances.[77]

U.S. policymakers must engage other countries in order to develop a system that will ensure the interoperability of the global system, but also meets the requirements of national security and law enforcement. Multilateral agreements must be reached if the U.S. policy goal of a key recovery (escrow) system is to become a reality. There is precedence for foreign nations entering into cooperation with regard to establishing regulations governing the export of items for military use. For instance, the Coordinating Committee (CoCom) was created as a Western response to the Soviet Union at the height of the Cold War. Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxembourg, the Netherlands, Norway, Portugal, Spain, Turkey, the United Kingdom, and the United States cooperated to attempt to prevent the Soviet Union from obtaining certain types of computers.[78] CoCom serves as a precedence for creating an arena for international cooperation with regard to cryptography.

The Future

The concepts and technology addressed in this analysis are likely to change in the next few years. Computer technology is constantly changing and progressing. Government and industry must work together to develop policies that adjust to changes in technology and enhance information security. Unfortunately, there has been an absence of such cooperation in the development of cryptography policy. A mechanism should be put in place to ensure that further policy discussions provide industry, law enforcement, private businesses, and government officials with an opportunity to consult each other. Channels of communication must remain open to ensure that a well-balanced policy, not a top-down government solution, is enacted.

The concepts and technology addressed in this analysis are likely to change in the next few years. Computer technology is constantly changing and progressing. Government and industry must work together to develop policies that adjust to changes in technology and enhance information security.

Topics for continued discussion among these different parties, as identified by Vice President Gore, include:

- evaluating the developing global key recovery architecture
- assessing lessons learned from key recovery implementation
- advising on technical confidence issues vis-a-vis access to and release of keys
- addressing interoperability and standards issues
- identifying other technical, policy and program issues for government action[79]

The new Clinton administration policy will only be in effect for two years, and then will be evaluated and/or changed. With the software industry, civil liberties organizations, and a growing number of legislators questioning the plan, the policy is on unstable ground. Cryptography policy is trapped in the mentality of protecting United States national security interests and the concerns of federal and local law enforcement. But, developing cryptography policy for the future of the global Internet necessitates a change of philosophy. Future cryptographic policy analysis must continue to progress beyond national security issues and consider the concerns of businesses and private citizens as they adjust to the ever-expanding Information Age.

Notes

[†]I would like to acknowledge all of the assistance given to me in the process of producing this article. This article would not be possible if not for the hard work of my article editor, Lynn Bagorazzi, and my associate editor, Mercy Viana, whom I thank for their help and advice. I'd also like to thank Rachel Mosher-Williams for hard work in getting the article finished and Professor Kasle for teaching me the art of being specific. Finally and most important, I owe the deepest debt of gratitude to my family for all of the sacrifices that they have made for my education.

[1] Kenneth Dam and Herbert Lin, "Cryptography's Role in Securing the Information Society," National Research Council (Washington, DC, 30 May 1996); available from http://www2.nas.edu/cstweb/2646.html; INTERNET.

[2] U.S. General Accounting Office, *Communication Privacy: Federal Policy and Actions* (Washington, DC: GAO/OSI-94-2, 4 November 1993), 1.

[3] *Ibid.*, 3.

[4] Richard Behar, "Who's Reading Your E-mail?" *Fortune*, 3 February 1997, 58-59.

[5] *Ibid.*

[6] U.S. GAO, *Communication Privacy*, 3.

[7] David E. Colton & G.A. Keyworth, "The Computer Revolution, Encryption and True Threats to National Security," The Progress and Freedom Foundation (Washington, DC, June 1996), available from http://www.townhall.com/pff/encry.html; INTERNET.

[8] Michael A. Froomkin, "The Metaphor is the Key: Cryptography, the Clipper Chip and, the Constitution," *University of Pennsylvania Law Review* 143 (1995): 724.

[9] Netscape Communications, Inc., Security Information Alert. The alert appears when users of the Netscape Navigator attempt to send information. The user has the option after the initial alert to either continue or cancel the transmission.

[10] *Phillip Karn, Jr v U.S. State Department and Thomas McNamara*, Brief of Amici Curiae, United States Court of Appeals for the District of Columbia No 96-5121 (7 October 1996); available from http://www.epic.org/crypto/export_controls/amicus_brief.html; INTERNET. In this case, Phillip Karn has filed suit over restrictions which prevent him from selling his programming language and cryptographic formulas on the grounds that such restrictions are a violation of the First Amendment guarantee of freedom of speech;

[11] Internet Architecture Board and Internet Engineering Steering Group, "IAB and IESG Statement on Cryptographic

Technology and the Internet 4," (24 July 1996); available from ftp://ftp.isi.edu/in-notes/rfcl984.txt; INTERNET.

[12] U.S. GAO, *Communication Privacy*. An algorithm is defined as, "A mathematical procedure that can usually be explicitly encoded in a set of computer language instructions that manipulates data." Six standard algorithms are generally discussed, Data Encryption Standard (DES), Skipjack, RC2, RC4, RSA and DSS. DES is the most widely used algorithm and uses 56-bit keys. RC2 and RC4 use 40-and 56-bit keys. Skipjack uses 80 bit keys.

[13] Jim Bidzos, Ian Goldberg, and Cipher Deavors, interview by Bobbi Battista, *CNN World Today*, CNN, 31 January 1997.

[14] *Ibid.*

[15] *Ibid.*

[16] *Ibid.*

[17] Alex Lash, "Gore Offers Strings-Attached Encryption Policy" (1 October 1996); available from C/Net News.com at http://www.news.com/News/Item/0,4,4003,00.html; INTERNET.

[18] Interview with Bidzos, Goldberg, and Deavors, interview by Battista.

[19] *Karn, Jr v U.S. State Department and Thomas McNamara*; INTERNET.

[20] Dam and Lin, "Cryptography's Role in Securing the Information Society"; INTERNET.

[21] Louis Freeh, Testimony before the House Judiciary Committee on International Terrorism, 6 April 1996; available from http://www.epic.org/crypto; INTERNET

[22] U.S. GAO, *Communication Privacy*, 9.

[23] *Ibid.*, 6. GAO points out, "The Computer Security Act of 1987 reaffirmed NIST as the responsible federal agency for developing federal cryptographic information-processing standards for the security of sensitive, unclassified information. However, NIST has followed NSA's lead when developing certain cryptographic standards for communications privacy."

[24] *Ibid.*, 12-13. In 1984, President Ronald Reagan signed National Security Decision Directive 145 that authorized the Director of the NSA to review and approve all security-related standards for informations systems, including those set by NIST. In March 1989, NSA and NIST sighed a Memorandum of Understanding that requires NIST to seek NSA's guidance "in all matters related to cryptographic algorithms." If NIST and NSA disagree, the matter is appealed to the Secretaries of Commerce and Defense.

[25] Dam and Lin, "Cryptography's Role in Securing the Information Society"; INTERNET.

[26] *Ibid.*

[27] *Ibid.*

[28] *Ibid.*

[29] *Ibid.*

[30] Interview with Bidzos, Golberg, and Deavors, interview by Battista.

[31] Louis Freeh, Testimony before the Senate Judiciary Committee, Subcommittee on Terrorism, 27 April 1995; available from http://www.epic.org/crypto; INTERNET.

[32] Internet Architecture Board and Internet Engineering Steering Group, "Internet Groups Critical of Government Proposals to Restrict Encryption Technology"; [cited April 1996]; available from http://inor.isoc.org/whatsnew/cryptog.html; INTERNET.

[33] *Karn, Jr v U.S. State Department and Thomas McNamara*; INTERNET.

[34] Honorable Tom Cambell, et. al., "Letter to the President of the United States," 15 May 1996; available from http://www.epic.org; INTERNET.

[35] U.S. GAO, *Communication Privacy*, 8.

[36] IBM, "The Need for a Global Cryptographic Policy Framework," An IBM Position Paper (1 December 1996); available from http://www.ibm.com/Security/crypto/html/pp_global.html; INTERNET.

[37] Dam and Lin "Cryptography's Role in Securing the Information Society"; INTERNET.

[38] David E. Colton and G.A. Keyworth, "The Computer Revolution"; INTERNET.

[39] *Katz v United States*, 389 U.S. 347, 353 (1967).

[40] *Karn, Jr v U.S. State Department and Thomas McNamara*; INTERNET.

[41] *Bernstein v U.S. State Department*, 922 F. Supp. 1426, 1439, (N.D. Cal 1996).

[42] Alex Lash, "Judge Rejects Crypto Limits" (9 December 1996); available from C/NET/NEWS.Com at http://www.news.com/News/Item/0,4,6343,00.html; INTERNET.

[43] *Ibid.*

[44] Dam and Lin, "Cryptography's Role in Securing the Information Society"; INTERNET.

[45] Conrad Burns, et al., "Letter to the Honorable Mickey Kantor, Secretary, Department of Commerce" (15 October 1996); available from http://www.epic.org/crypto/key_escrow/clipper4_cong_letter.html; INTERNET.

[46] Bill Summary & Status for the 104th Congress, S. 1726 [cited 5 February 1997]; available from http://thomas.loc.gov; INTERNET.

[47] Honorable Tom Campbell, "Letter to the President of the United States"; INTERNET

[48] Alex Lash, "Gore Offers Strings-Attached Encryption Policy"; INTERNET.

[49] Reuters Ltd, "Clinton Administration to Offer Encryption Bill Shortly," 20 March 1997.

[50] Center for Democracy and Technology, "End of Session Wrap-Up of Crypto Policy Reform Efforts - A CDT Policy Post" (31 October 1996); available from Intellectual Capital.com at http://www.intellectualcapital.com/icpolicy2.html; INTERNET. The CDT claims, "As the Clinton Administration continues to push its plans to satisfy law enforcement concerns, the Internet commmunity must be ready to work hard to protect privacy and security on the Internet."

[51] Joint Press Announcement, "High-Tech Leaders Join Forces to Enable International Strong Encryption" (2 October 1996); available from http://www.epic.org/crytp/key_escrow/joint_announce_ 10_2_96.html; INTERNET.

[52] *Ibid.*

[53] *Ibid.*

[54] Alex Lash and Courtney Macavinta, "Did Crypto Industry Get Wonked?" (11 December 1996); available from C/NET/NEWS.com at http://www.news.com/News/Items/0,4,6135,4000.html?related; INTERNET.

[55] Vice President Al Gore, "Statement of the Vice President," The White House, Office of the Vice President (1 October 1996); available from http://www.epic.org/crypto; INTERNET.

[56] Alex Lash, "Industry Fights Crypto Rules"; INTERNET.

[57] U.S. Department of Commerce, Bureau of Export Administration, "Department of Commerce Encryption Export Regulations," *Federal Register*, Volume 61, Number 251 (30 December 1996): 68572-68587.

[58] Reuters Ltd, "Clinton Administration to Offer Encryption Bill Shortly," 20 March 1997. The Administration plans to introduce legislation that would affirm the liberal use of cryptography domestically. No explicit law is currently on the books. The bill will involve the introduction of a voluntary key escrow system and would outline legal considerations for release of the keys and criminalizes misuse of they keys.

[59] President William Jefferson Clinton, Executive Order, "Administration of Export Controls on Encryption Products" (15 November 1996); available from http://www.epic.org/crypto; INTERNET.

[60] Alex Lash, "Gore Offers Strings-Attached Encryption Policy"; INTERNET.

[61] Senator Patrick Leahy, "Statement of Sen. Patrick Leahy on 'Key Recovery' Proposal" (1 October 1996); available from http://www.epic.org/crypto; INTERNET.

[62] Interview with Bidzos, Goldberg, and Deavors, interview by Battista.

[63] Alex Lash and Courtney Macavinta "Did Crypto Industry Get Wonked?"; INTERNET.

[64] *Ibid.* In a letter to Vice President Gore described in this article, the BSA outlined 5 things which BSA expects to be implemented in the new rules: (1) Companies should not be required to participate in the key escrow system; (2) The government should lift all export restrictions on encryption products in a key recovery system; (3) The government should let companies develop a key escrow system at their own pace; (4) The government should allow for export of 56-bit encryption sorftware, even if the vendor does not have a key escrow system; and (5) The government should allow all encryption products to work together regardless of whether the vendors participated in key recovery.

[65] Conrad Burns, "Burns Cautions on Encryption Plan: Statement from Senator Conrad Burns on 'Key Recovery' Proposal" (1 October 1996); available from http://www.epic.org.; INTERNET.

[66] *Ibid.*

[67] Dam and Lin, "Cryptography's Role in Securing the Information Society"; INTERNET.

[68] *Ibid.*

[69] *Ibid.*

[70] *Ibid.*

[71] *Ibid.*

[72] Joint Press Announcement, "High-Tech Leaders Join Forces to Enable International Strong Encryption"; INTERNET.

[73] Dam and Lin, "Cryptography's Role in Securing the Information Society"; INTERNET.

[74] *Ibid.*

[75] Conrad Burns, "Burns Cautions on Encryption Plan; INTERNET.

[76] Dam and Lin, "Cryptography's Role in Securing the Information Society, Appendix G"; INTERNET.

[77] IBM, "The Need for a Global Cryptographic Policy Framework"; INTERNET.

[78] Dam and Lin,"Cryptography's Role in Securing the Information Society, Appendix G"; INTERNET.

[79] Al Gore, "Statement of the Vice President."

Bibliography

Behar, Richard. "Who's Reading Your E-mail?" *Fortune*, 3 February 1997, 58-59.

Bernstein v U.S. State Department, 922 F. Supp. 1426, 1439. (N.D. Cal 1996).

Bidzos, Jim, Cipher Deavors, and Ian Goldberg. Interview by Bobbi Battista. *CNN Today*, 31 January 1997.

Bill Summary & Status for the 104th Congress. S. 1726. Available from http://www.thomas.loc.gov.; INTERNET.

Burns, Conrad. "Burns Cautions on Encryption Plan: Statement from Senator Conrad Burns on 'Key Recovery' Proposal." 1 October 1996. Available from http://www.epic.org; INTERNET.

Burns, Conrad, et al. "Letter to the Honorable Mickey Kantor, Secretary, Department of Commerce." 15 October 1996. Available from http://www.epic.org/crypto/key_escrow/clipper4_cong_letter.html; INTERNET.

Campbell, Honorable Tom, et.al. "Letter to the President of the United States." 15 May 1996. Available from http://www.epic.org; INTERNET.

The Center for Democracy and Technology. "End of Session Wrap-Up of Crypto Policy Reform Efforts - A CDT Policy Post." 31 October 1996. Available from Intellectual Capital.com. IC Policy Online 2: Crypto Policy Reform Efforts at http://www.intellectualcapital.com/icpolicy2.html; INTERNET.

Clinton, William Jefferson. " Executive Order: Administration of Export Controls on Encryption Products." 15 November 1996. Available from http://www.epic.org; INTERNET.

Colton, David E., G.A. Keyworth. "The Computer Revolution, Encryption and True Threats to National Security." June 1996. Available from The Progress and Freedom Foundation at http://www.townhall.com/pff/encry.html; INTERNET.

Dam, Kenneth, and Herbert Lin. "Cryptography's Role in Securing the Information Society." National Research Council, 30 May 1996. Available from http://www2.nas.edu/cstweb/2646.html; INTERNET.

Freeh, Louis. Testimony before the Senate Judiciary Committee, Subcommittee on Terrorism. 27 April 1995.

_____. Testimony before the House Judiciary Committee on International Terrorism. 6 April 1996.

Froomkin, A. Michael. "The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution." *University of Pennsylvania Law Review*,143 (1995): 724.

Gore, Albert. Statement of the Vice President. Washington DC: Office of the Vice President, 1996.

IBM. "The Need for a Global Cryptographic Policy Framework: An IBM Position Paper" [cited April 1996]. Available from http://www.ibm.com/Security/crypto/html/pp_global.html; INTERNET.

Internet Architecture Board, Internet Engineering Steering Group. "IAB and IESG Statement on Cryptographic Technology and the Internet 4." 24 July 1996. Available from ftp://ftp.isi.edu/in-notes/rfc1984.txt; INTERNET.

_____. Press Release: "Internet Groups Critical of Government Proposals to Restrict Encryption Technology." Available from http://www.inor.isoc.org/whatsnew/cryptog.html; INTERNET.

Joint Press Announcement. "High-Tech Leaders Join Forces to Enable International Strong Encryption." 2 October 1996. Available from http://www.epic.org/crypto/key_escrow/joint_announce_10_2_96.html; INTERNET.

Katz v United States. 389 U.S. 347, 353 (1967).

Lash, Alex. "Gore Offers Strings-Attached Encryption Policy." 1 October 1996. Available from C|Net News.com at http://www.news.com/News/Item/0,4,4003,00.html; INTERNET.

_____. "Industry Fights Crypto Rules." 31 December 1996. Available from C|Net News.com at http://www.news.com/News/Items/0,4,6560,00.html; INTERNET.

_____. "Judge Rejects Crypto Limits." News.com December 19, 1996. Available from C|Net News.com at http://www.news.com/News/Item/0,4,6343,00.html?related; INTERNET.

Lash, Alex, and Courtney Macavinta. "Did Crypto Industry Get Wonked?" 11 December 1996. Available from C|Net News.com at http://www.news.com/News/Items/0,4,6135,4000.html?related; INTERNET

Leahy, Patrick. "Statement of Sen. Patrick Leahy on 'Key Recovery' Proposal." 1 October 1996. Available from http://www.epic.org/crypto; INTERNET.

Philip R. Karn, Jr v U.S. State Department. Brief of Amici Curiae. Electronic Privacy Information Center, American Civil Liberties Union Foundation, National Headquarters; Internet Society and U.S. Public Policy Committee of the Association For Computing Machinery. United States Court of Appeals for the District of Columbia No 96-5121. Available from http://www.epic.org/crypto/export_controls/amicus_brief.html; INTERNET.

Reuters Ltd., "Clinton Administration to Offer Encryption Bill Shortly," 1997.

U.S. Department of Commerce, Bureau of Export Administration, "Department of Commerce Encryption Encryption Export Regulations." *Federal Register*, Vol. 62, No. 251 (30 December 1996): 68572-68587.

U.S. Government Accounting Office. "Communication Privacy — Federal Policy and Actions." No. GAO/OSI-94-2. 1993. Available from http://www.thorplus.lib.purdue.edu:8100/gpo/G...20/diskb/wais/data/gao/os94002; INTERNET.