Policy Analysis

No. 325 November 19, 1998

ENCRYPTION POLICY FOR THE 21ST CENTURY
A Future without Government-Prescribed Key Recovery

by Solveig Singleton

Executive Summary

Encryption technology encodes computer files so that only someone with special knowledge, such as a unique secret "key," can read them. The widespread use of strong encryption technology is essential to protect consumers and businesses against spies, fraud, and theft over the computer networks used in electronic commerce.

The federal government has just announced a new policy that will maintain restrictions on the export of encryption stronger than 56 bits. Stronger encryption technology may be exported only to subsidiaries of U.S. companies in most countries, or to certain economic sectors in 42 countries (insurance, health, banking, or online merchants), or if the exporter builds in a key-recovery infrastructure that will enable law enforcement officers to access the secret keys.

Some law enforcement interests support legislation that would force U.S. citizens and residents to give the government access to their keys. Government-prescribed key recovery and export controls are a grave danger to the privacy of law-abiding citizens and businesses, not only in the United States but around the world. And the development of the key-recovery infrastructure might well be technically impossible and would be prohibitely expensive.

Export controls and government-prescribed key recovery will not keep strong encryption out of the hands of criminals and terrorists, because the technology is readily available worldwide without key-recovery features. Law enforcement interests should explore other options for dealing with strong encryption. Recent calls for "balance" make enticing sound bites (who would be opposed to "balance?") but compromise the freedom to innovate and sacrifice vital civil liberties.

Solveig Singleton is director of information studies at the Cato Institute.

Cryptography has been used for centuries to secure private communications using codes and ciphers.[1] Julius Caesar used a cipher in which every letter was replaced by the letter that occurred three letters later in the alphabet, so "ATTACK AT DAWN" became "DWWDFJ DW GDZQ."[2] Today, encryption software or hardware can mix up the bits of data sent over computer networks, so that only those with the private key to the cipher can break it.

Understanding the debate about whether to regulate encryption has become vital to discussions of international trade, domestic economic policy, computer network security, privacy, and the future of the limits on government power set by the U.S. Constitution.

This paper examines the two faces of the current regulatory regime export controls and government-approved "key escrow" requirements. It concludes that the existing regulations that persist in spite of recent reforms are untenable. The cost of the regulatory regime is tremendous, the benefits speculative at best.

Pressure to regulate the use of strong encryption comes from law enforcement interests.[3] Strong encryption may be unbreakable by law enforcement within a reasonable period of time (though some experts suspect that the government has understated its ability to crack those codes).[4] Strong encryption thus can make wiretaps less useful.

What almost all law enforcement interests want is "key escrow" or "key-recovery" mandates. Under this system, people who use encryption must file their secret keys with the government or another third party, or include decoding information along with the message, so that the police can decode their messages without their knowledge. Whit Diffie and Susan Landau compare key escrow to "the little keyhole in the back of the combination locks used on the lockers of school children. The children open the locks with the combinations . . . but the teachers can always look in the locker using the key."[5] Law enforcement interests want access not only to stored messages but to communications as they actually occur (called "real time" access).

Law enforcement interests argue that unbreakable encryption shifts the "balance" of law enforcement and privacy interests established by the Fourth Amendment toward individual privacy. Federal Bureau of Investigation director Louis Freeh testified that "the unchecked proliferation of non-key-recovery encryption will drastically change the balance of the Fourth Amendment in a way

which would shock its original proponents."[6] Attorney General Janet Reno has said that encryption with special access for law enforcement would "make sure that the technology, as used, complies with the Constitution."[7]

But the idea that unbreakable encryption is beyond the comprehension of the framers and does not "comply with the Constitution" is wrong. Cryptography was well known to participants in the American Revolution, including James Madison, John Adams, Ben Franklin,[8] George Washington, John Jay,[9] James Lovell,[10] and Benedict Arnold, who designed the code he used to betray his country. History demonstrates that modern computer technology is not the only way to create a virtually unbreakable encryption system.[11] Thomas Jefferson created a cipher strong enough to be used by the U.S. Navy until 1967.[12] The Vignère cipher was considered unbreakable at the time of the American Revolution.[13] But the Constitution as written does not restrict private citizens' use of encryption.

Throughout history, the science of cryptography repeatedly advanced beyond the ability of cryptanalysts to crack the codes. While, law enforcement officers have always had the right to <u>try</u> to decipher encrypted messages, <u>they have never had a practical or constitutional guarantee of success</u>. The government's right to search one's house does not entail "a power to forbid people to hide things."[14]

With that historical backdrop in mind, this paper outlines the debate over encryption policy to show where encryption policy has been and where it is going. The paper addresses the following issues:

- how encryption technology works;
- why we need very strong encryption;
- why we need privacy against powerful governments, as well as private-sector hackers;
- the history of encryption regulations, from the Clipper Chip to recent liberalization proposals;
- the impact and efficacy of remaining export controls;
- government-prescribed key-recovery infrastructure; and
- current legislative proposals.

The conclusion assesses the probable outcome of any further attempt to ensure that everyone participates in a government-prescribed key-recovery system. For years law enforcement interests have pushed for a system of international and domestic controls, under which users of strong encryption within the United States must guarantee that the government can access their secret keys. Two forces are opposed--the power of technology driven by market demand and the power of government, backed by sheer force. In the end, technology will win, bringing a new age of prosperity as well as new dangers.

This paper leaves a critical issue for another day--how the First Amendment, which protects our rights to communicate with one another as we choose, or the Fourth Amendment, limits the government's power to regulate encryption.

One preliminary issue remains: Can one fairly represent law enforcement's interests in this debate without access to classified information? Yes. Thirteen of 16 National Research Council committee members reviewed classified information pertinent to the debate. They concluded that "the debate over national cryptography policy can be carried out in a reasonable manner on an unclassified basis."[15] That is fortunate because arguing with people who cannot share what they insist is vital information on the topic is pointless.

An Overview of Encryption Technology

Encryption software or hardware uses a mathematical algorithm to scramble bits of data sent or stored on computer networks. The key to the cipher is a string of numbers or other characters. The stronger the algorithm and the longer the string, the harder it is to break.

The length of a key is measured in "bits," the number of digits in the key. For most encryption techniques in widespread use today, the bit length of the key can be used as an approximation of the strength of an encryption program. Longer bit length does not guarantee greater security; a poorly designed security program could be invaded without the invader's making a "brute force" attack on the key (a "brute force" attack consists of trying all the possible keys before finding the one that fits). But longer bit length usually means stronger encryption.[16]

Caesar's cipher used the simplest form of encryption, known as "secret key" or "symmetric" encryption. To decipher the message, the recipient must know the same formula the sender used to scramble the message to begin with--that is, the encrypting formula and the secret key are identical. But the sender might have no secure way to communicate the secret key to the recipient of the message. And the recipient might reveal the key to someone else, or use the key to forge a document in the sender's name.

The development of "public key" encryption from 1974-1975 solved those problems. There are two keys, a public key and a private key; the relationship between the two keys is determined by a nearly insoluble mathematical problem.[17] The public key is available to anyone who wants it and may be printed in a directory or posted on the Internet. The private key is known only to the individual user. Anyone who wants to send a message to that user encrypts the message with the user's public key. Only the user's private key can decrypt the message.

Public key cryptography provides a way for the recipient of a message to identify the sender, a "digital signature." The sender encrypts part of the message, the signature, with his or her private key. The recipient decrypts this part with the sender's public key, confirming the sender's identity. Digital signatures will be important to the successful growth of Internet commerce; for example, banks will want to be certain that they are actually communicating with their customers, and the customers will want to be certain that they are communicating with their banks.[18]

When both the recipient and the sender are using public key technology, encryption can provide privacy and identity authentication. The sender signs a message with his private key and enciphers the message with the recipient's public key. The recipient deciphers the message with her private key and checks the sender's signature with his public key.

Perhaps the best-known public key software available is Pretty Good Privacy, which offers the equivalent of 128-bit security. PGP was created by Phil Zimmermann in 1991 to protect the privacy of e-mail. Shortly after its release, a researcher in Germany received a copy through an anonymous remailer and posted PGP on the Internet.[19] Today, there are more than 3.5 million users of PGP around the world.[20] The most recent version, PGP 5.5, has been posted anonymously on the Internet by "unknown Cypher-

punks."[21] Believing that the spread of PGP violated U.S. law, the U.S. Customs Service initiated a three-year investigation of Zimmermann, which finally ended without indictment in January 1996.

Public key cryptography amounts to a revolution in security because it enables computer users to secure and authenticate their communications without revealing their own secret keys. The general cryptographic system can be exposed to public scrutiny, allowing weaknesses to be ferreted out, as long as the key remains secret.[22] Attempts to regulate encryption technology that undercut that fundamental advance are likely to be unpopular with users.

Why the Market Will Not Trust 56 Bits

Although encryption is not sufficient to secure information on computer systems, it is still necessary. Encryption will be necessary to ensure the privacy and integrity of private letters, phone calls, medical records, attorney-client communications, tax forms transmitted electronically, anonymous digital cash, bank transactions,[23] trade secrets, intellectual property,[24] and databases with sensitive information such as credit records. It is also necessary to protect information infrastructure such as electric power grids and airline navigation systems, which might be a target of information warfare or terrorism. But how strong must encryption be to be trusted with our credit card numbers, medical records, or messages generated by the next Paul Revere? Is 56 bits--strong enough now and for the future?

Keys of 40 bits were widely used because stronger keys could not be legally exported, but many successful "hacks" showed that a 40-bit key is clearly not strong enough now and certainly will not be strong enough in the future.[25] The administration recognizing this, has abandoned its plan to allow export under general license of 40-bit encryption only as of January 1, 1999.[26]

The administration's new proposal, announced September 16, 1998, would continue to allow export of 56-bit encryption without a license after a one-time technical review. Many companies use a 56-bit encryption algorithm known as Data Encryption Standard (DES), developed by International Business Machines (IBM) and the National Security Agency (NSA) in the 1970s.[27] One early analysis predicted that by 1996, an agency or company willing to invest $300,000 in off-the-shelf technology could crack DES in a mere 19 days.[28] This theory has since become a hard reality. In

July 1998, cryptographers John Gilmore and Paul Kocher broke the 56-bit DES code in 56 hours using a single PC to control an array of chips; the entire assembly cost $250,000.[29] But DES can also be broken for little or no cost, as demonstrated by Rocke Verser, whose volunteer network of 14,000 computer users linked over the Internet broke the DES code in June 1997.[30] RSA Labs' RC5 56-bit key was also broken in October 1997 by a network of 4,000 teams using computing power equivalent to more than 26,000 Pentium 200s.[31]

Given the widespread publicity of this feat, even if 56 bits would stop most casual hackers most of the time, the market has lost its trust in thls level of technology; it cannot provide a foundation for the trusted infrastructure of electronic commerce.[32] The industry standard is now triple DES, which uses DES 3 times with three different keys.[33]

Bit lengths must continue to grow longer. The problem is Moore's law, which states that the power of a microprocessor doubles approximately every 18 months, while costs stay the same.[34] Advances in mathematics can also make existing encryption obsolete,[35] and breaking keys has become a "sport" among young cryptographers.[36]

Encryption used today must be very strong indeed if it is to remain effective.[37] Whit Diffie and six other cryptographers report that to protect information adequately for the next 20 years, keys should be at least 90 bits long. For today, they recommend keys of 75 bits (which as of January 1996 would take 6 years and 70 days to crack).[38] The message revealed when Gilmore and Kocher cracked the DES code was "It's time for those 128-, 192-, and 256-bit keys."[39]

Encryption and the Future of Human Rights

The above section illustrates why we need encryption to guard against malicious 12-year-olds or glowering fanatics with bombs in their luggage.[40] Perhaps the most dangerous potential invaders are governments, however. In many countries today and, historically, in every country including the United States, many citizens fear and feared their own governments. Encryption is a powerful weapon against oppression worldwide.

More than 7,500 human rights groups worldwide combat torture, mysterious disappearances, and government massacres by disseminating information such as reports of

witnesses of government brutality. Email is a powerful tool. In 1988 the murder of Chico Mendes in Brazil was reported globally over the Internet even before it was published in newspapers. Flooded by telegrams and faxes, the Brazilian government arrested and convicted the killers.[41] In 1993 three leaders of the Russian Labor Party opposed the Russian government's attack on a Moscow television station. They were arrested and deprived of basic procedural rights. Minutes after the situation was reported over the Glasnet Network, the police were inundated with telephone calls from around the world, and the three were freed within hours.[42]

Such activity has brought human rights groups into grave danger from the governments whose activities they report, and many groups operate in the face of constant surveillance. More than 70 countries worldwide use widespread, uncontrolled, or illegal wiretaps.[43] Often, the taps target journalists, political opponents, and human rights workers; in 1991, for example, wiretaps and hidden microphones were found at the Mexican Human Rights Commission.

Patrick Ball of the American Association for the Advancement of Science reports that

> every year, many human rights workers are . . . captured, tortured and killed . . . so that their captors can obtain information from them. Quite often the captors are government agents. . . . Computers are also vulnerable to capture.[44]

Human rights groups must use strong encryption to defeat surveillance, protecting the content and authenticity of electronic messages. In Guatemala, a database holding the names of witesses to military slaughters is encrypted, as is a South African database keeping the names of applicants for amnesty for apartheid-related crimes.[45] Human rights workers used encryption to keep Argentinian intelligence forces from reading confidential messages passing between Spain and Argentina during the trial of Argentinian military in Spain for "disappearing" Spanish citizens.[46]

Phil Zimmermann's stated motive in inventing PGP was to ensure that citizens had a means to escape heightened surveillance by abusive governments.[47] His distributed PGP as freeware, saying, "I wanted cryptography to be made available to the American public before it became illegal to use it. I gave it away for free so that it would achieve wide dispersal, to inoculate the body politic."[48]

Today, PGP is used by human rights groups worldwide, including Amnesty International and other witnesses reporting human rights violations in Ethiopia, the Balkans, Burma,[49] Guatemala, and Tibet. On the day Boris Yeltsin shelled the Russian Parliament, Phil Zimmermann received an email from someone in Latvia, saying, "Phil I wish you to know: let it never be, but if dictatorship takes over Russia your PGP is widespread from Baltic to Far East now and will help democratic people if necessary. Thanks."[50]

Law enforcement argues that encryption gives the private citizen too much privacy from the police. Historically, however, humanity has never been as vulnerable to electronic surveillance as it is today. Virtually absolute privacy has always been a possibility since the beginning of history. Two or more people could enjoy a completely private conversation by going to the middle of a plowed field, where they could be certain that no one could overhear them.[51] Wax seals protected the privacy of envelopes, allowing recipients to detect tampering with the envelope.

Today, electronic eavesdropping methods allow law enforcement officers to invade that zone of total privacy. Many of the methods used are alternatives to wiretaps that are not defeated by the use of encryption, including[52]

- improved call-tracing methods;
- surveillance with infrared scanners;
- aerial surveillance;
- bugging;
- filters that pick certain voices[53] or keywords out of the babble of telecommunications traffic, formerly precluded by the sheer volume of calls;[54]
- supersensitive satellite photography that lets the police peer into our windows;[55]
- vast electronic databases;
- plaintext readers such as Tempest, which let police read the text appearing on computer screens through closed doors and walls; and
- laser light beams that allow conversations to be deduced from the vibrations of a windowpane.

Internet transactions such as credit card purchases, e-mail, and clickstream data provide a wealth of new ways for law enforcement authorities to employ electronic surveillance methods.

As a result, the balance of power is tipping away from individual liberty in favor of law enforcement.[56] Wiretapping alone rigged the game in favor of law enforcement.[57] Security technologies threaten a "Big Brother" future of omnipresent telephone monitoring. New encryption technology merely lets privacy catch up with law enforcement.

Most citizens of most countries do not have the luxury of trusting their governments. What does that mean for encryption regulation? First, regulations enacted under the assumption that we can trust law enforcement and other officials worldwide and within the United States to do the right thing can endanger our freedoms and civil rights. Second, for encryption regulations to work at all, they must be enacted by every country. That means giving the keys to humanity's private communications to tyrants, disabling one of the most potent weapons against oppression ever devised.

Trends in Encryption Regulation

While some aspects of the encryption regulatory regime have been altered over the years, the goal of the people in charge of making encryption policy remains the same--to ensure the creation of an infrastructure that guarantees the government's ability to decode encrypted messages--both within the United States and abroad.[58]

Export Controls until 1996: The 40-Bit Limit

Legislators have long used export controls to keep military technology out of the hands of enemies of the United States. Because encryption has military uses, those also applied to encryption.[59] Ultimately, regulation of encryption came under the Arms Export Control Act of 1976 (AECA).[60] Under AECA, encryption was regulated by the State Department, pursuant to the International Traffic in Arms Regulations (ITAR).[61] ITAR classed encryption as a "munition" on the U.S. munitions list.

If the State Department exempted an encryption product from the munitions list,[62] the product was then regulated by the Commerce Department as a "dual-use" product under

the Export Administration Act of 1979 (EAA). The EAA spawned the Export Administration Regulations (EAR). The EAA expired in 1994, but the EAR have been continued by executive orders of questionable validity declaring a perpetual state of "emergency."[63]

As of late 1996, under ITAR, encryption software that used a key length of more than 40 bits could be exported only with the permission of the National Security Agency. Banks were allowed to use some cryptography products offering 56-bit protection. Export of up to 64-bit-long products was permitted if the exporter ensured that government could access the keys.

Recent Key Escrow and Key-Recovery Initiatives

Regulators offered to relax the export controls--if the software designers would build encryption that gave the government access to users' private keys. Each proposal along those lines has failed miserably, only to be replaced by another proposal with mainly cosmetic differences.[64] Recent liberalization measures, however, show that the whole fabric of regulation is collapsing.

Clipper I and Clipper II. In 1993 law enforcement and national security agencies proposed "that cryptography be made available and required which contains a 'trap door' that would allow law enforcement and national security officials, under proper supervision, to decrypt enciphered communications."[65]

Though that proposal was never enacted into law, the same year the administration adopted the "Clipper Chip" as the federal government's encryption standard, hoping that the government's purchasing power would be sufficient to set a market standard for domestic and international use. Clipper is an 80-bit encryption algorithm designed by the National Security Agency. Law enforcement could access the plain text of any Clipper-enciphered communications, because critical key information would be kept in "escrow" with the Department of Commerce and the Treasury Department.[66] The administration proposed lifting export controls on companies that use Clipper. To describe the Clipper plan as unsalable would be a understatement; the proposal now hangs like an albatross around the administration's neck.

In 1995 the administration substituted key escrow for Clipper (dubbed Clipper II). Under that proposal, strong encryption technology could be exported if exporters filed

the key with government-certified escrow agencies. That proposal, like the original Clipper, failed to attract private-sector support.

Clipper III, The Key Management Infrastructure. On May 17, 1996, the Clinton administration's Interagency Working Group on Cryptography[67] proposed the creation of a "key management infrastructure" (KMI). Under that plan, trusted certification authorities would certify that a certain public key was really registered to a certain individual or corporation. But no one would be permitted to participate in the KMI unless he escrowed his key with a trusted party (such as the certification authorities).[68] Encryption technology could be exported as long as the keys were safely escrowed somewhere, perhaps with a foreign government that had agreed to cooperate with the United States.[69] That proposal, dubbed "Clipper III," immediately faced heavy opposition.[70]

On July 12, the White House released a statement[71] emphasizing that individuals and businesses would need to give their keys to a trusted third party, "as many people do with their house keys," so they would have a spare key in the event that their own key was lost.[72] The administration promised "temporary" relief from export controls.[73]

At that time, administration officials began to abandon the use of the very unpopular term "key escrow" and began to use the term "key recovery" or "key management" instead.

Too Little, Too Late: Partial Relaxation of Export Controls

In the fall of 1996 the Clinton administration announced that it would allow companies to export key lengths of up to 56 bits under a general license, but only if the companies agree to incorporate key escrow (now dubbed "key recovery") features within two years. The general export license would be valid for six months and would be renewed if the company could show "progress in developing a key-recovery plan."[74] Vice President Gore explained that exporters would be required to commit to developing key-recovery features and to building the supporting infrastructure for key recovery.

> Initial approval will be contingent on firms providing a plan for implementing key recovery. The plan will explain in detail the steps the applicant will take to develop, produce, distrib-

> ute, and/or market encryption products with key-recovery features.[75]

But by 1999, nothing stronger than 40 bits would be exportable without government-approved key-recovery features.[76] The new policy applies to both hardware and software products.

The plan also moves jurisdiction over encryption from the State Department to the Bureau of Export Administration at the Commerce Department.[77] For the two-year period, encryption stronger than 56 bits may, as before, be exported only under special exemptions.[78] After the two-year period, "no key length limits or algorithm restrictions would apply to exported key-recovery products."[79]

The vice president described key recovery as a system whereby "a trusted party (in some cases internal to the user's organization) would recover the user's confidentiality key for the user or for law enforcement officials acting under proper authority. Access to keys would be provided in accordance with destination country policies and bilateral understandings."[80]

Initially, the new policy (the 56-bit limit) seemed to be a strategic success for the administration, if only because 11 major corporations[81] agreed to participate in developing key-recovery plans. That (grudging)[82] support enabled Secretary of Commerce Mickey Kantor to declare victory:

> The administration's encryption plan is reasonable, workable, fair and coherent. . . . The proof that our plan will with the critical mass of industry that has announced its intention to work with the administration to develop a key-recovery system, which will allow law enforcement, under proper court order, to have access to encrypted data.[83]

Support from that "critical mass of industry," quickly evaporated.[84] One important issue involved the definition of key recovery. If there was no difference between "key recovery" and "key escrow," why had the administration abandoned the use of "escrow" in favor of "recovery"? The change was to all appearances a deliberate obfuscation. Eventually "officials . . . let it be known that there is no real difference between key recovery and key escrow."[85] Industry representatives had thought that key recovery would enable users to recover lost keys without necessarily requiring users to deposit their keys with third par-

ties or allowing law enforcement to access the plain text (unencrypted text) of messages in real time (as opposed to the plain text of stored messages).[86] There were other substantial grounds for disagreement as well.

Nevertheless, the administration moved onward, releasing new encryption regulations in interim form on December 30, 1996, to take effect January 1, 1997.

The Current Regulatory Scheme

The current regulations cover technology (information that can be used to manufacture, use, or reconstruct encryption products), encryption software, and software designed to create or use encryption software. The rules allow the export of the object code of mass market products with 40-bit strength or less after a one-time seven-day review. Products of up to 56-bit key length that do not support key recovery may be exported during the two-year window if the manufacturer makes a satisfactory commitment to develop key recovery. Key-recovery products may also be exported. Advance access to plaintext would have to be given to a government-approved third party in order for key-recovery products to gain approval. The requirement would apply to real-time communications as well as stored data. Approved products could not be interoperable with products that did not offer key access. Exporters would be required to submit detailed business plans and product designs for initial government scrutiny, and undergo additional scrutiny every six months.[87] Encryption software that does not necessarily give users the ability to encode the information in a document, such as signature software and virus checkers, is also subject to the new rules.

The rules do allow the export of source code or object code published in a book or other media.[88] But the interim regulations also state that "the administration continues to review whether and to what extent scannable encryption source or object code in printed form should be subject to the EAR and reserves the option to impose export controls on such software for national security and foreign policy reasons."[89]

Furthermore, the rules attempt to control not only the export of technology to a foreign country but its reexport from that country. If a technology contains any amount of encryption technology developed in the United States--no amount is considered de minimis[90]--reexport is subject to controls.[91] While the operation of the de min-

imis rule is far from clear, it seems to undermine the exemption for printed source code.

While the current rules, unlike ITAR, restrict the time the Commerce Department and its multiple advisers have to make an initial licensing decisions, there are apparently no set time limits on the procedures for appeal if the license is denied, except for a note that the procedure must take a "reasonable time."[92] The Department of Justice and the CIA have been added as reviewing agencies under the new scheme.

The current rules, like ITAR, control "technical assistance" to foreign nationals in using cryptography;[93] that also undermines the exemption for printed materials. Also, with respect to encrpytion software, the rules do not exempt publicly available software, educational materials, or fundamental research.[94] The regulations generally exempt teaching activities,[95] but not if undertaken with an improper intent. Thus, like ITAR and for the same reasons, the rules restrict academic researchers' communications with foreign colleagues or students.

September, 1998: A Sectoral Liberalization Proposal

On September 16, 1998 the Clinton administration announced an export control liberalization measure for some users of encryption products. The new policy will permit the export of up to 56-bit encryption after a one-time review. Export of products with unlimited bit length will be permitted to subsidiaries of U.S. companies worldwide, except for those in Iran, Iraq, Libya, Syria, Sudan, North Korea, and Cuba.[96] Products of unlimited bit length with or without key recovery will be permitted to online merchants in 45 countries for client-server applications (affecting, for example, Secure Socket Layer encryption),[97] and to banks, health and medical organizations, financial companies, and insurance companies in those 45 countries. This exception does not include biochemical/pharmaceutical manufacturers.[98] Exports of products that support key recovery (or similar features, such as Cisco's "private doorbell" products)[99] will be given a presumption of approval for export to 42 countries. These approvals will be issued under license after a one-time review; prior review of the identity of the foreign key recovery agent is eliminated,[100] as is review of six-month key recovery progress reports.[101] This liberalization proposal is a sign that the wall of regulation is crumbling. The technology has been unleashed, and the technology is winning.

Domestic Encryption Controls

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

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

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

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

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

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

"Balance" and Compromise

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

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

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

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

- offers no relief for the sale of point-to-point encryption products like PGP, which encrypt messages on the user's computer, and

- offers no relief for the sale of real-time encryption products, which encrypt your files as you work on them.[113]

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

The Effect and Efficacy of Export Controls

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

Unilateral or Universal Controls?

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

This necessary condition for the success of export controls does not hold for encryption. A bare handful of countries, mostly undemocratic ones such as Belarus, China, Pakistan, and Russia, impose domestic controls on the use of encryption. France and the United Kingdom can expect pressure to lift their policy of supporting key access to conform with the policy of the European Union.[116] While members of the European Union do license the export of cryptography, they have strongly resisted enforcing those controls as strictly as the United States[117]--opposing, for example, the requirement that exported products support key escrow.[118] Many countries do not and are not expected to have export controls. The vast majority of countries offer safe havens for the manufacture, use, and distribution of encryption and are expected to continue to do so.[119]

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

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

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

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

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

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

The Burden of Export Controls to Individual Companies

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

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

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

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

```
Export policy

Software-Version:                          Mozilla/4.0P3

PKCS12-DES-EDE3:                           false

PKCS12-DES-56:                             false

PKCS12-RC2-40:                             true

SSL2-RC4-128-WITH-MD5:                     false

SSL2-RC2-128-CBC-WITH-MD5:                 false

SSL2-DES-168-EDE3-CBC-WITH-MD5:            false

SSL2-RC4-128-EXPORT40-CBC-WITH-MD5:        true

SSL3-FORTEZZA-DMS-WITH-RC4-128-SHA:        false

SSL3-RSA-WITH-RC4-128-MD5:                 conditional

SSL3-RSA-WITH-RC2-CBC-40-MD5:              true
```

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

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

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

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

Export Control's Impact on Domestic Security

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

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

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

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

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

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

The Futility of Export Controls

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

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

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

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

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

The impact of the 40 bit limit is illustrated by a case involving Netscape. A large corporation in Germany considered using Netscape's 128 bit key software to establish a sophisticated national health-care data network based on "smart cards." Netscape, however, could not provide the software because of export controls. So the German government had a German company build the software from scratch. "This not only means a loss of a sale to Netscape. It also means that a new competitor has been created where one did not exist before."[143] The new sectoral reforms mean that this problem may not occur again with health care, but instead with biochemical or pharmaceutical manufacturing.

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

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

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

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

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

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

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

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

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

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

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

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

The National Research Council lists several other evasion techniques, including

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

What's Left for Law Enforcement?

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

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

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

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

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

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

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

A Closer Look at Key Recovery

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

The Limited Private-Sector Need for Key Recovery

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

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

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

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

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

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

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

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

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

The Implausibility of Proposals for Key-Recovery Infrastructure

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The Dangers of Government Abuse

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

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

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

target political opponents, including William Safire and Joseph Kraft.[174]

Evasion of the Fourth Amendment has often threatened our civil liberties. High-ranking government officials have declared that even if evidence garnered from illegal wiretaps cannot be used in court, the evidence gathered by that means can be so valuable for intelligence purposes that illegal wiretaps should still be used.[175] Even seemingly legitimate sources of data such as census and tax records have substantial potential for abuse; such information infrastructure should not be permitted to grow further.

In the last analysis, it is dangerous to permit the government to dictate an infrastructure and industry standards that could allow law enforcement to invade our privacy almost at will, should the political winds shift.

Espionage by Foreign Governments. Many foreign governments, including those of "friendly" countries like Japan, France, and Britain, are engaged in espionage.[176] The FBI views economic espionage by foreign intelligence services as "a significant threat to U.S. national security."[177] The danger of government abuse is made more acute by the participation of foreign governments in key-recovery infrastructure. If the United States wants other countries to give its law enforcement officers access to keys to aid U.S. authorities in enforcing U.S. laws, other countries will expect the United States to turn over keys to aid them in enforcement of their laws.

The United States may find that it has committed to participate in an infrastructure than entails grievous human rights violation. If, for example, a human rights worker has escrowed a key in the U.S. but violates a foreign law against sedition by reporting what the foreign government is up to, must the U.S. escrow agent turn over the key to the foreign government? And a U.S. citizen whose communications cross national boundaries will get little protection from the Fourth Amendment. There would be little to stop foreign agencies from manufacturing excuses to obtain keys escrowed in the United States in order to conduct government-sponsored espionage.

Even if every government agrees that the police can only access keys with a warrant based on probable cause that a crime was committed, this provides no protection from governments that have no compunction about turning any harmless act into a crime.

The Future of Encryption Legislation

A number of bills have been proposed to reform the rules for exporting encryption technology.[178] The Security and Freedom Through Encryption (SAFE) Act, (H.R. 695), introduced by Rep. Bob Goodlatte (R-Va.) and Rep. Zoe Lofgren (D-CA),[179] has won substantial support in the House. The Secure Public Networks Act, (S. 909), represents another type of bill, purporting to protect the right to use non-key-recovery products while tilting the economic incentives in favor of participation in government-certified key-recovery systems, and maintaining a strict regime of export controls. Justin Matlick's report, "U.S. Encryption Policy: A Free-Market Primer," contains an excellent analysis of these bills.[180] The most recent bill as of this writing is the Encryption Protection the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY Act, (S. 6027).[181] Important features common to one or more of these bills are discussed below.

Allowing Export of Mass-Market Encryption

SAFE and several other measures, including the E-PRIVACY Act, are intended to liberalize export controls by allowing the export of encryption technology in the public domain or is generally available. This would be a step forward, but only a tiny step.

While at least the "public availability" test avoids the hopeless problem of trying to limit key lengths, it leaves developers of cutting edge technology, particularly academics engaged in research, out in the cold. Or would we have the other side of the coin--any technology could be exported merely by being posted to the Internet and thus become "public" with the flick of a few keys? Defining export-able technology by reference to its public availability is circular.

The E-PRIVACY Act would allow the unlicensed export of encryption that provides comparable security to a product that is or will be available outside the United States from a foreign supplier. Again, the intent is laudable. But as with "generally available," just what products would be "comparable" or "available" from foreign suppliers is open to question. The E-PRIVACY Act refers the question to a "Encryption Export Advisory Board," a bureaucratic solution probably worse than no solution at all. Also, the provision dooms U.S. developers to follow foreign developers in innovation and market development.

Finally, the E-PRIVACY Act falls short in continuing to require encryption exporters to submit products to the Department of Commerce for review.

Prohibitions on Mandatory Key Escrow

Vice President Gore has asserted that "domestic use of key recovery will be voluntary, and any American will remain free to use any encryption system domestically."[182] A number of bills would prohibit "mandatory" key escrow. But most would not expressly preclude mandatory "voluntary" key escrow introduced by substantial arm-twisting, including

- requiring recipients of federal subsidies to develop and use key escrow,
- requiring certification authorities to escrow keys, and
- federal intervention in standard-setting processes.

For example, the Clinton administration's Clipper III proposal stipulated that no one would be permitted to participate in the Key Management Infrastructure (KMI) unless he escrowed their key with a trusted party such as the Certification Authorities.[183] The report still described key escrow under those circumstances as "voluntary," although attempts to use encryption outside the KMI would be stymied without the aid of certification authorities to help users determine with whom they are dealing on the network. Key escrow, the report claimed, would occur "naturally" under these conditions.[184]

A tightly regulated key-recovery infrastructure that exists only because of the exercise of government power is hardly "voluntary." Government has many types of power, and the exercise of this power in any form constrains and distorts choices made by consumers and by the industry.

The E-PRIVACY bill addresses this issue by specifically barring the federal government from using its purchasing power or intervention with standard-setting to block the spread of non-escrow encryption. The bill also requires the United States to purchase encryption products that interoperate with non-escrow products.

Tying Key Recovery to Digital Signatures or Certification Authorities

Many observers assert that the development of electronic commerce will require trusted "certification authorities," third parties to a transaction that can certify to customers that a certain public key or digital signature is in fact that of a real business and not an electronic imposter. If government action is required either to establish certificate authorities or the validity of digital signatures, government standards for either could foist key recovery on an unwilling market. Because the private section will and should lead the way in recognizing digital signatures and establishing certificate authorities, however, any attempt to leverage government involvement with certification or authentication into mandatory key recovery will fail.

First, there is no good reason for anyone's use of a certificate authority to be tied to their willingness to escrow his or her secret keys. There is no sound reason that a user's secret key should ever leave his or her control.[185] Supporters of mandatory key recovery once proposed making anyone's use of certification authorities contingent on their willingness to escrow their key with a government-approved agent.[186] But certificate authorities are not a desirable place for keys to be stored or generated. Users should generate and store their own public and private keys, not rely on a third party to do so. The third party would have to transmit the key pair to the user, exposing it to theft. And the third party would store the keys, adding to risks of theft and fraud.

Because there is no need for government to be involved in establishing certificate authorities, however, the threat of tying certificate authorities to key escrow has diminished. Some argue that legislation is needed to protect certification authorities from liability in the event that someone fraudulently obtains or uses a certificate of identity. But certification authorities could limit their liability by contract. The main obstacle to this is that some courts will not respect the parties' freedom to contract to limit liability. So far, in any event, theoretical threats of liability have not prevented certificate authorities from taking off in the private sector.

The private sector is leading the way. Certification simply requires a trusted third party such as a bank to attest that a certain public key really belongs to a certain business or individual. Verisign, Inc., a spin-off

of RSA, already provides such services, as does Thawte, the South African security product company.[187]

Also, note that many electronic transactions will not require certification. Different business communities require different levels and types of trust to proceed. Businesses need not know the identity of their consumers; they only need know that they will be paid. Anonymous digital cash provides business with this assurance without certification. And some digital cash is traceable by the consumer who spends the cash (not anyone else), protecting the consumer against fraud without certification.

The debate over the validity of digital signatures might provide supporters of mandatory key escrow with other opportunities to do mischief. The debate over the validity of electronically communicated signatures is nothing new; it raged in the 19th century over the validity of teletyped or telegraphed initials, was taken up again when oral contracts began to be made by telephone, and still later when the courts considered whether to accept faxed signatures. In each case, ultimately, the electronically communicated agreements came to be considered valid--the courts considered the matter, and let business custom lead the way. The private sector and then the courts can be trusted to assess when digital signatures should be recognized, just as they did with telegraphs,[188] telephones,[189] telexes,[190] faxes,[191] or photocopies of signatures,[192] or audio recordings.[193] In 1869, one court explained that a telegraphed contract was valid, saying:

> It makes no difference whether that operator writes the offer or the acceptance . . . with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by the use of the finger resting upon the pen; nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office.[194]

As long as the technology is reliable, there is no reason a court would not say the same of digital signatures. Thus it is doubtful whether legislation such as S. 2107, the Government Paperwork Elimination Act, which requires agencies of the federal government to accept and allows them to establish standards for digital signatures, is necessary.[195] Indeed, the bill may be dangerously premature.

Lessons of History: How Encryption Controls Will Fail

Export controls and mandatory key recovery are doomed to fail. The goal of law enforcement interests is an extraordinarily ambitious one--to regulate an entire medium or language of communication simply because a few messages among millions might possibly result in a harm--harm that could be prevented by other means. The closest historical analogy is to Henry VIII's insistence on licensing the printing press, on the grounds that some of the presses, some of the time, might be used to print treasonous or heretical matter.

In the wake of problems with heresy, comprehensive formal licensing of the press began in 1526 when the Bishop of London and the Archbishop of Canterbury were made the sole licensers of all books.[196] Faced with political and religious dissension, in 1528, Henry VIII began to regulate the access of foreigners to the printing trade. He issued a decree barring foreign printers from setting up any new shops and from employing more than two alien servants.[197] In 1529, Henry VIII issued a list of banned books.[198] The Act of 1534 banned the sale of foreign books in England, except by the King's Stationer.[199] In 1538, the king announced a regular system of licensing to control all printing, "for expellinge and avoydinge the occasion of errours and seditiouse opinions."[200] The Puritans moved a secret press around England to produce religious tracts in 1588 and 1589.[201]

The licensing system was perpetuated by later laws such as the Licensing Act of 1692. Of this law, Trenchard and Gordon protested that licensing of the press "subjects all learning and true information to the arbitrary will and pleasure of a mercenary, and perhaps ignorant licenser; destroys the properties of authors in their copies; and sets up many monopolies."[202] Exactly the same might be said of encryption regulations. Both encryption controls and Henry VIII's press licensing restricted an entire communications technology, neutral in itself, because a very few people might use it to break the law.

Today we recognize licensing of the press as a wholly illegitimate and oppressive regime. That is precisely how future generations will look upon encryption export controls.

Conclusion

As Peter Huber has pointed out, 1984 was a better year than Orwell ever expected.[203] Instead of "Big Brother" surveillance, we have myriad intelligent nodes, in their sheer number and complexity apparently resistant to centralized control. The future is not here yet, however. A decentralized network could prove more of an instrument of oppression than a centralized one, if the police establish a presence at every node.

To the law-abiding citizen in a free and peaceful country, law enforcement officers are an essentially benign force. To the law enforcement community, however, everyone is a potential suspect. If this view drives the making of encryption policy, we will no longer have a free country. By then, it will be too late for the law-abiding citizen to remember what citizens of China, Burma, and other oppressive countries cannot forget. Law is not always just, law enforcement officers can be as cruel and arbitrary as other human beings, and legal guarantees of privacy can mean little or nothing in the face of a gun.

This is why the battle over encryption standards and infrastructure and protocols, the fabric of electronic commerce, is critically important. Legal restraints on the authority of the police such as the Fourth Amendment are important, but they are not enough if the infrastructure facilitates social control. "Compromise" approaches to problems for law enforcement created by encryption and compression technology, such as export controls coupled with key escrow, err on the side of Big Brother.

But the export control policy is doomed, with or without a "key-recovery" option.

- Over today's instantaneous networks, regulation of encryption can be evaded almost without effort.

- Markets will inexorably demand simple, cheap, and universal security solutions--but export controls and key recovery make essential security technology costly and complicated.

- Driving encryption innovation overseas and underground will only make the task of law enforcement harder.

What will replace this policy? The most likely possibility is a world where strong encryption is freely available, inexpensive, and exportable. The technology would

converge towards a world-wide standard. Some users, probably large commercial enterprises, would have some kind of key-recovery system in place for stored data. Few individual users would.

What does this mean for law enforcement? Wiretapping would become less useful. Freeh presents this as a new problem, saying that "police soon may be unable through legal process and with sufficient probably cause to conduct a resonable and lawful search or seizure, because they cannot gain access to evidence being channeled or stored by criminals, terrorist, and spies."[204] As a practical matter, police have always encountered difficulties with encryption. Even informal codes such as street slang can pose insurmountable difficulties for the police.[205]

Law enforcement officers have many alternatives to wiretapping, including the use of bugs and informants. Descrambling technology could advance to the point where "unbreakable" encryption becomes breakable again. The United States also could conduct its foreign policy with the goal of lowering the risk of terrorism to the public.[206]

The alternative to a world where encryption is freely available is a system of universal or almost universal controls. Every government would control the export and perhaps import of encryption technology, and insist on a key-recovery framework for exportable technology. Oppressive regimes anxious to control dissident activity would embrace these controls enthusiastically. Encryption technology would be too complicated and expensive for most users. Systems developed in different countries would not work well together.

A gray market in non-escrow encryption products would spring up, perhaps centered in the United States, where export and import controls would be successfully challenged by academics urging respect for rights of free speech. The non-escrow technology would easily spread anonymously across the Internet, posted to university networks and on public computers. Soon, anyone who wanted to bypass the key-recovery infrastructure would be free to do so. The vast majority of those who ignored the system, especially in this country, would never be caught or prosecuted. Wiretapping would become less useful, especially as law enforcement grappled with a myriad unstandardized double and triple-layered encryption techniques. Other law enforcement techniques such as infiltration of terrorist or criminal groups would have to take its place. Descrambling technology could advance.

The future is coming, either way. The question remaining is how much time and money bureaucrats will waste on our way there.

Notes

1. To use a code, both parties to the message must agree beforehand what a certain sequence of symbols will mean. A cipher, by contrast, can be used to scramble any message.

2. Steven Levy, "Battle of the Clipper Chip," New York Times Magazine, June 12, 1994, pp. 44, 47.

3. For further description of law enforcement concerns, see National Research Council, Computer Science and Telecommunications Board, CRISIS: Cryptography's Role in Securing the Information Society (Washington: National Academy Press, 1996), p. 89 (cited hereafter as NRC).

4. A panel of private crypto experts concluded that it would take two minutes to crack 56-bit DES on a $30 million machine; the National Security Agency estimated it would take one year and 87 days. Private communication from George Spix to author, June 17, 1997; see also G. A. Keyworth, II, and David E. Colton, "The Computer Revolution, Encryption and True Threats to National Security," Progress and Freedom Foundation, Future Insight, June, 1996, p. 7.

5. Whitfield Diffie and Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption (Cambridge, Mass.: The MIT Press, 1998), p. 6.

6. Louis J. Freeh, director, Federal Bureau of Investigation, Testimony before the Senate Judiciary Committee, July 9, 1997, p. 4, http://www.epic.org/crypto/legislation/freeh_797.html; see also Louis J. Freeh, Statement of July 25, 1996, before the Committee on Commerce, Science, and Transportation, United States Senate, http://www.epic.org/crypto/ exports_controls/freeh.html.

7. Quoted in Declan McCullagh, "Afternoon Line," Netly News, March 19, 1998, http://www.cgi.pathfinders.com/netly/article/0,2334,13212,00.html.

8. In 1775, Charles Dumas, employed as a foreign agent by what was to become the United States, provided Ben Franklin with a cipher he used for secret correspondence

while he lived outside Paris. Ralph E. Weber, "James Lovell and Secret Ciphers during the American Revolution," Cryptologia 2, no. 1 (January 1978): 75.

9. John Jay designed a cipher used in correspondence between himself and Robert Livingston. Ibid., p. 85.

10. James Lovell signed the Articles of Confederation, serving as a delegate to the Continental Congress.

11. David Kahn, The Codebreakers (New York: Macmillan, 1967), pp. 192-95. Indeed, Lovell hoped that he had succeeded in creating an unbreakable cipher, saying in a letter to Abigail Adams, "I chalenge [sic] any body to tell the Contents truly." Weber, p. 78. Lovell's ciphers were extremely cumbersome and difficult to decipher, even by the intended recipients. His writing style for enciphered messages is intended to prevent decryption, using strange phraseology so as to confuse the would-be cryptanalyst. Ibid., p. 83.

12. Kahn, pp. 192-95.

13. Ibid., pp. 214-21.

14. Diffie and Landau, p. 228.

15. NRC, p. 4 (emphasis in original).

16. A cryptographic algorithm is considered strong if

> 1. there is no shortcut that allows the opponent to recover the plain text without using brute force to test keys until the correct one is found and
>
> 2. the number of possible keys is sufficiently large to make such an attack infeasible.

Matt Blaze et al., "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security," January, 1996, http://www.bas.org/policy/encryption/cryptographers.html, p. 2.

17. For example, to generate the public key, two very large prime numbers are multiplied to get a larger number. Depending on the length of the numbers and the speed of available computer equipment, it could take billions of years for a would-be code cracker to factor this product, that is, figure out which numbers were multiplied together to get the larger number, and thus derive the private key. See generally Diffie and Landau, pp. 36-38.

18. "Any Time, Anywhere," Financial Times, September 5, 1996, p. 19; see also Timothy Tomlinson, "Contracts over the Internet Pave the Way for a Host of New Woes," Computer Law Strategist, June, 1997, pp. 1, 3.

19. A. Michael Froomkin, "The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution," University of Pennsylvania Law Review 143 (1995): 750.

20. Pardhu Vadlamudi, "Two U.S. Firms Are Dueling over Encryption Technology," Investor's Business Daily, June 19, 1997, p. A6.

21. See ftp://ftp.replay.com/pub/crypto/incoming /PGP55.zip.

22. Diffie and Landau, p. 13.

23. For a discussion of an attempted electronic theft of $400,000 from Citicorp, see NRC, p. 23; and Diffie and Landau, p. 42.

24. See NRC, p. 31.

25. For example, the exportable version of Netscape used 40 bit encryption. A French graduate student at the Ecole Polytechnique in Paris broke the 40-bit cipher in the summer of 1995 using an array of 120 workstations and some parallel computers to mount a brute-force attack; the key was found after about eight days. Undergraduates at the Massachusetts Institute of Technology used a single graphics computer to find the key in eight days. In late January 1997, Ian Goldberg, a UC Berkeley graduate student, penetrated RSA's 40-bit code in just three and a half hours, using 250 machines on Berkeley's network of workstations. Graeme Browning, "Top Secrets," National Journal, September 14, 1996, p. 1955; See also NRC, Box 4.5, p. 124.

26. "Administration Updates Encryption Policy," http://www.cdt.org/crypto/admin/whousepress091698.html, p. 1.

27. Diffie and Landau, pp. 24, 60.

28. Blaze et al., p. 7.

29. John Markoff, "US Data Code Is Unscrambled in 56 Hours," New York Times, July 17, 1998, p. C1.

30. Lloyd Chrein, "Anatomy of a Crack: How a Grass-roots Effort Broke the Encryption Code for Finanical Transactions," Pathfinder, June 20, 1997, p. 1.

31. Adam L. Beberg, Jeff Lawson, and David McNett, Letter to Alex Bischoff, October 22, 1997.

32. See Diffie and Landau, p. 27.

33. Ibid., p. 28.

34. In 1984 a desktop computer could execute 2 million instructions per second, but by 1994 the same machine was capable of 256 million instructions per second. By 1998 a desktop will run more than 2 billion instructions per second. Keyworth and Colton, p. 4.

35. Today, it is very difficult for anyone to derive a secret key from someone's public key, only because there are mathematical operations that are easy to perform in one direction and difficult to perform in the opposite direction. It is easy to multiply two large prime numbers together but hard to factor a huge number into constituent prime numbers. Advances in mathematics could change this. But a new type of strong encryption is already on the horizon--methods that use encryption based on quantum physics to alert parties to a conversation if anyone is eavesdropping. Bruce Dorminey, "Cryptographers Crack It: Quantum Physics Offers Secure Codes," Financial Times, March 18, 1997, p. 16.

36. Diffie and Landau, p. 27.

37. For a discussion of the lifetimes of cryptographic systems, see ibid., p. 28.

38. Blaze et al., p. 7.

39. Markoff, p. C1.

40. See Robert Uhlig, "Hackers Start Blackmailing Internet Firms," Electronic Telegraph, July 7, 1997, http://www.telegraph.co.uk:80; and Andrew Ross Sorkin, "2 Popular Web Sites Report Breaches in Their Security: Credit Card Numbers Exposed at Starwave," New York Times, July 10, 1997, p. D6.

41. "Human Rights Protection on the Internet," http://www.gilc.org/news/gilc-ep-statement-0198.html.

42. Ibid.

43. In the United States, the FBI monitors computer networks used by activist groups. In France, during the 1980s, intelligence agents monitored journalists and the opposition party. In the United Kingdom, British intelligence monitors activists and civil liberties groups.

44. Declaration of Patrick Ball, ACLU of Georgia v. Miller, Civil Action No. 96-CV-2475-MHS (January 24, 1997), http://www.aclu.org/issues/cyber/censor/gapbaffidavit.html.

45. Ibid.

46. "Human Rights Protection on the Internet."

47. "If we do nothing, new technologies will give the government new automatic surveillance capabilities that Stalin could ever have dreamed of. The only way to hold the line on privacy in the information age is strong cryptography." Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology and Space of the U.S. Senate Committee on Commerce, Science and Transportation, June 26, 1996, http://www.cdt.org/crypto/current_legis/960626_zimm_test.html.

48. Ibid.

49. Levy, p. 60.

50. Zimmermann.

51. An old Hebrew proverb warns, "Never tell a secret in a field full of little hills."

52. For a discussion of alternatives to wiretapping, see Economists Incorporated, DRAFT: Economic Framework for Analyzing the Costs and Benefits of Government-Mandated Key Recovery Systems (Washington: Economists Incorporated), pp. 9-10. See generally, Froomkin, "The Metaphor Is the Key," pp. 823-24.

53. Ibid., pp. 709, 806.

54. See NRC, p. 31.

55. The Central Intelligence Agency used satellite photographs to keep an eye on anti-war demonstrations; the Environmental Protection Agency has also used satellites to enforce pollution laws. David Burnham, The Rise of the Computer State (New York: Random House, 1980), pp. 46-47.

56. Zimmermann explains that the slow art of flyfishing for suspects has given way to driftnet technology:

> In the past, if the government wanted to violate the privacy of ordinary citizens, it had to expend a certain amount of effort to intercept and steam open and read paper mail, and listen to and possibly transcribe spoken telephone conversation. This is analogous to catching fish with a hook and a line, one fish at a time. Fortunately for freedom and democracy, this kind of labor-intensive monitoring is not practical on a large scale. Today, electronic mail is gradually replacing conventional paper mail. . . . E-mail messages are just too easy to intercept and scan for interesting keywords. This can be done easily, routinely, automatically, and undetectably on a grand scale. This is analogous to driftnet fishing--making a quantitative and qualitative Orwellian difference to the health of democracy, (p. 2).

57. Olmstead v. United States, 277 U.S. 438, 476 (1928)("As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping.")(Brandeis, J., dissenting).

58. "Administration Updates Encryption Policy," p. 1.

59. The Arms Export Control Act of 1949, intended to regulate munitions, also covered encryption. Congress also enacted the Mutual Security Act of 1954, which authorized the president to control the export of "arms, ammunition and implements of war, including technical data related thereto."

60. 22 U.S.C. Section 2778.

61. 22 C.F.R. Sections 120-30 (1996).

62. The State Department could remove a given encryption product from the U.S. Munitions List be classifying it as “dual-use” technology, that is, technology that was considered commercial as well as military in application.

63. A. Michael Froomkin, "Postscript," http://www.oaw.miami.edu/~froomkin/articles/planent_clipper.html#POSTSCRIPT.

64. In 1991, the FBI sought to include a "trap-door" provision in an anti-terrorism measure (S. 266). Providers of electronic communications services and equipment manufacturers would have been required to ensure that the systems permitted "the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law." Congressional Record (January 24, 1991), S1191.

65. Froomkin, "The Metaphor Is the Key," p. 809 n. 422.

66. See A. Michael Froomkin, "It Came from Planet Clipper: The Battle over Cryptographic Key 'Escrow,'" University of Chicago Legal Forum 15 (1996): 27. See also Comment, "The Clipper Chip: How Key Escrow Threatens to Undermine the Fourth Amendment," Seton Hall Law Review 25 (1995): 1142.

67. Interagency Working Group on Cryptography Policy, "Achieving Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure," May 17, 1996, pp. 4-6. Cited hereafter as Clipper III Draft Proposal.

68. Ibid., p. 5.

69. Government agencies would be able to obtain escrowed keys pursuant to government-to-government agreements. Ibid., p. 7. "There is a concern that U.S. products with keys escrowed in the U.S. will not be saleable overseas. Hence, it may be possible to permit overseas escrow in Europe, even before government-to-government arrangements are completed. This exception is possible since the European countries are already moving to implement key escrow systems." Ibid., p. 8.

70. See Center for Democracy and Technology, "Preliminary Analysis of 'Clipper III' Encryption Proposal," May 21, 1996. A report released by the National Research Council on May 30, 1996, supported the partial relaxation of export controls on encryption, arguing that the benefits of the widespread use of strong encryption would outweigh the costs. See generally NRC.

71. Albert Gore, "US Cryptography Policy: Why We Are Taking the Current Approach," July 12, 1996.

72. "The encryption key would be provided voluntarily by a computer user to a trusted party who holds it for safe keeping. This is what many people do with their house keys--give them to a trusted neighbor who can produce them when something unexpected goes wrong. Businesses should

find this attractive because they do not want to lock up information and throw away the key or give an employee--not the company--control over company information. An individual might also use this service to ensure that she can retrieve information stored years ago." Ibid., p. 1.

73. The statement added that we should not "damage our own national security . . . by spreading unbreakable encryption, especially given the international nature of terrorism. Even 40 bit encryption, if widespread and not escrowed, defeats law enforcement." Ibid.

74. Computer and Communications Industry Association, "Administration Revises Encryption Policy," CEO Report, October 10, 1996, p. 1. Cited hereafter as CCIA Report.

75. Albert Gore, "Statement of the Vice President," October 1, 1996, p. 1, http://cdt.org/crypto/clipper311/9161001_ Gore_stmnt.html.

76. CCIA Report, p. 1.

77. David E. Sanger, "Clinton Ready for Exports of Data Codes," New York Times, October 1, 1996, p. D1. Encryption products intended for military purposes remain under the jurisdiction of the State Department.

78. Longer key lengths will continue to be approved for products dedicated to the support of financial applications.

79. Gore, p. 1.

80. Ibid.

81. See Apple Computer, Atalla, Digital Equipment Corporation, Groupe Bull, Hewlett-Packard Company, IBM, NCR Corp., RSA, Sun Microsystems, Inc., Trusted Information Systems, and UPS, "High-Tech Leaders Join Forces to Enable International Strong Encryption," Joint press announcement, October 2, 1996, p. 1. Cited hereafter as Joint press announcement.

82. "Export controls are a fact of life," explained Jim Bidzos, president of RSA and a longtime foe of regulatory restrictions on encryption. "The Key Recovery Alliance's approach will allow companies to use cryptography with differing levels of security in an interoperable way. When the alliance implements this technology it will give the user a new flexibility that did not exist before. In an imperfect world this technique will at least allow you

to take advantage of what governments around the world will allow." Ibid., pp. 3-4.

83. Michael Kantor, "The Administration's Encryption Plan," Letter to the editor, Washington Post, October 18, 1996, p. A26.

84. The Key-Recovery Alliance, an international industry group founded to discuss voluntary key recovery, initially supported the administration's plan. Two months after declaring its willingness to support the new 56-bit limit policy, the Business Software Alliance, whose members included many of administrations policy's initial 11 supporters and member's of the Key-Recovery Alliance, such as Apple, changed its mind. In December 1997, Network Associates Inc., now owner of PGP Inc., withdrew from the Key-Recovery Alliance.

85. Michael S. Lelyveld, "Software Firms: Clinton 'Backtracking,'" Journal of Commerce, December 5, 1996, p. 3A.

86. See Joint press announcement, p. 2; Robert W. Holleyman, II, president of the Business Software Alliance, Letter to The Honorable Albert Gore, December 2, 1996; Becca Gould, vice president, Public Policy, Business Software Alliance, Letter to Mr. Bruce McConnell, Information Policy & Technology, OMB, and to Mr. Ed Appel, National Security Council, November 8, 1996.

87. Department of Commerce Encryption Export Regulations, Interim Rules, Federal Register, 61, no. 251 (December 30, 1996): 68572-87. Cited hereafter as Interim Rules.

88. Ibid., p. 68578, Sec. 734.3, 734.7.

89. Ibid.

90. Encryption technology does not lose its U.S. origin when "redrawn, used, consulted, or otherwise commingled abroad in any respect with other software or other technology. . . . Therefore, any subsequent or similar software or technology prepared or engineered abroad for the design, contruction, operation, or maintenance of any plant or equipment, or part thereof, which is based on or uses any such U.S.-origin software or technology is subject to the EAR." Ibid., Sec. 734.4 (b)(h).

91. Export now includes "an actual shipment or transmission," or "release to a foreign national in the United States," or downloading, or causing the downloading of,

such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the United States, or making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photooptical, photoelectric, or other comparable communications facilities accessible to persons outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites, unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States. The rules also broaden the definition of export to more clearly encompass posting material on the Internet. Ibid., Sec. 734.2.

92. 15 C.F.R. 756.2(c)(1).

93. The rules explain that "the EAR also restricts technical assistance by U.S. persons with respect to encryption commodities or software." Interim Rules, p. 68577, section 730.5; see also William J. Clinton, Executive, Order, November 15, 1996, p. 2 http://samsara.law.cwru.edu/comp_law/ThePressRelease.html. The interim draft of the new regulations also contains Sec. 736.2(7), according to which U.S. persons may not engage in "certain financing, contracting, service, support, transportation, freight forwarding, or employment that you know will assist in certain proliferation activities." According to Bruce Kurtz, export policy analyst, Office of Strategic Trade and Foreign Policy Controls, this section was intended to apply only to nuclear bombs and missiles; however, the section's inclusion in the encryption regulations seemed to make this unclear. Email from Lucky Green to cypherpunks@toad.com, December 31, 1996.

94. Interim Rules, pp. 68578-79, Sec. 734.3, Sec. 734.8, Sec. 734.9.

95. No U.S. person may, without a license from BXA, provide technical assistance (including training) to foreign persons with the intent to aid a foreign person in the development or manufacture outside the United States of encryption commodities and software. Note in addition that the mere teaching or discussion of information about cryptography, including, for example, in an academic setting, by itself would not establish the intent described in this section, even where foreign persons are present. Ibid., pp. 68572-87, p. 68584, Sec. 744.

96. "Administration Updates Encryption Policy," p. 1.

97. "Fact Sheet: Administration Updates Encryption Policy," http://www.epic.org/crypto/ export_controls/wh-factsheet-998.html, p. 1 (hereafter "Fact Sheet").

98. Ibid.

99. "Press Briefing by the Vice President," September 16, 1998, http://www.epic.org/crypto/export_controls/wh-transcript-998.html, p. 5.

100. "Fact Sheet," p. 1.

101. "Press Briefing by the Vice President," September 16, 1998, p. 4.

102. The National Research Council recommends against domestic limits. NRC, pp. 264, 303.

103. Gore, "Statement of the Vice President," p. 1.

104. See proposed amendment to the SAFE Bill by Rep. Ben Gilman (R-N.Y.), drafted on July 21, 1997, "Amendment to H.R. 695, as amended by the subcommittee on International Economic Policy and Trade,"http://www.cdt.org/crypto./legis_105/SAFE/970725_prop.html (outlawing the import or sale within the United States of products that do not support real-time decryption); see also FBI director Freeh's stipulation that one bill, S. 909, did not go far enough as it supports only voluntary key escrow and adding that "export controls on encryption products exist primarily to protect national security and foreign policy interests. However, law enforcement is more concerned about the significant and growing threat to public safety and effective law enforcement that would be caused by the proliferation and use within the United States of a communications infrastructure that supports strong encryption products but cannot support timely law enforcement decryption." Freeh, Testimony, p. 3.

105. Quoted in Rajiv Chandrasekaran, "Freeh Seeks Encryption Decoding Key," Washington Post, September 4, 1997, p. E1.

106. Epstein said,

> The system introduces a massive sytem of potential surveillance. It cuts out the notice and knock provisions that must be satisfied before a warrant could be executed. It vests vast powers

> in third-party agents who have neither the incentive nor knowledge to contest any government intrustion. It presupposes uniform good faith by public officials and overlooks the major costs of even a tiny number of official misdeeds or mistakes.

Richard A. Epstein, testimony before the Senate Judiciary Subcommittee on the Constitution, Federalism, and Property Rights, March 17, 1998, p. 6. Professor Michael Froomkin of the University of Miami School of Law explains that "the Fourth Amendment does not give the government an affirmative right to an effective search." Froomkin, "The Metaphor Is the Key," pp. 826. He concludes that the Fourth Amendment probably prohibits warrantless mandatory key escrow, at least for private, noncommercial users of encryption. Ibid., p. 833.

107. Senator Lott explains that domestic controls on encryption would "invade our privacy; be of minimal use to the FBI; would require nonexistent technology; woud create new administrative burdens; and would seriously damage our foreign markets," http://jya.com/lott-crypto.htm.

108. Congressional Record, November 7, 1997, p. S11959, statement of Senator Ashcroft. (S. 909 gives the FBI "unprecedented and troubling" authority to invade lives).

109. John J. Hamre, "Information Assurance, Encryption Policy, and National Security," Journal of Information Policy 1 no. 1 (June 1998): 10-13, p. 12.

110. The proposal was called "private doorbell" to distinguish it from the FBI's demand for escrow of the "house key."

111. The companies are Ascend, Bay Networks, 3Com, Hewlett-Packard, Intel, Microsoft, Netscape, Network Associates, Novell, RedCreek Communications, Secure Computing and Sun Microsystems. "Thirteen High-Tech Leaders Support Alternative Solution to Network Encryption Stalemate," http://www.cisco.com/warp/public/146/july98/3.html.

112. Declan McCullagh, "Cisco Backs Backdoor for Internet Wiretaps," Netly News, July 14, 1998, http://cgi.pathfinder.com/netly/article/0,2334,14025,00.html; and Jim Kerstetter, "High-Tech Group Offers Crypto Plan," PC Week Online, July 13, 1998, http://www.zdnet.com/pcweek/news/0713/13ecrypt.html.

113. See Benjamin Keyser, "Data Fellows to Enable Real-Time Encryption," InfoWorld, June 8, 1998, p. 66.

114. National Academy of Sciences, Scientific Communication and National Security (1982)(Corson Report) p. 65.

115. Edmund L. Andrews, "Europeans Reject U.S. Plan on Electronic Cryptography," New York Times, October 9, 1997, p. D4.

116. See Jennifer L. Schenker, "French Proposal for Encryption Is Worrying EC," Wall Street Journal, October 20, 1997, p. B11.

117. Until 1996, international trade in encryption was regulated by the Coordinating Committee for Multilateral Export Controls (COCOM). COCOM has permitted the export of mass-market encryption products since 1991. In 1996, COCOM was superseded by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Its rules for export of encryption are similar to COCOM. Jesse S. Casman, "Internet Cryptography: Does Japan Have a Role?" Japan Policy Research Institute Occasional Paper no. 12, March 1998, p. 4.

118. See Ibid.

119. Ibid.; and Will Rodger, "Ireland Takes Hands-Off Stand on Crypto," Interactive Week, July 27, 1998, p. 40.

120. The United Kindom's home secretary announced a new initiative to give police access to private encryption keys in February 1998, contradicting the Labour Party's earlier manifesto:

> We do not accept the 'clipper chip' argument developed in the United States for the authorities to be able to swoop down on any encrypted message at will and unscramble it. The only power we would wish to give to the authorities, in order to pursue a defined legitimate anti-criminal purpose, would be to enable decryption to be demanded under judicial warrant.

"Global Internet Liberty Campaign Member Statement: New UK Encryption Policy Critised," February 1998, p. 2.

121. The Japanese government encouraged Japanese companies to seize the initiative in exploiting international markets for strong encryption products. Nippon Telegraph &

Telephone Corp., the Japanese electronics giant, announced it would begin selling computer chips with 128-bit keys. Mitsubishi Electric has developed a 128-bit code, and Hitachi has reportedly developed encryption programs that produce a 256-bit key. Browning, p. 1955. Nippon Telephone began producing chips that use a triple-DES algorithm and one with the RSA public key. Used together, the chipset could produce a key length of 1024 bits. In late 1996, however, the Clinton administration successfully urged Japan to adopt export controls more like those of the United States. It remains to be seem whether these limits will be enforced. Japanese researchers continue to work hard on cutting-edge encryption technology, such as "elliptic curve encryption." Casman, p. 2.

122. Global Internet Liberty Campaign, "Cryptography and Liberty: An International Survey of Encryption Policy," February 1998, p. 7.

123. "Towards a European Framework for Digital Signatures and Encryption," p. 16, http://www/ispo.cec.be/eif/ policy/97503.html#I.

124. Quoted in Brooks Tigner, "EU Aims to Spur Encryption Trade by Lifting Limits," Defense News, October 13-19, 1997, p. 94.

125. "CCIA's Black Chats Encryption with VP," Computer and Communications Industry Association CEO Report, August 22, 1997, p. 1.

126. See Fred M. Gregaras and Rogerm M. Golden, "Access to U.S. Software and Other U.S. Technology by Foreign Nationals," http://www.okoumene.com/ softwacces_exprt.html.

127. Computer and Communications Industry Association, "Encryption Policy Update I," October 1996.

128. Computer and Communications Industry Association, "Senators Interested in Quick Action on Encryption Bill," CEO Report, June 9, 1997, p. 2.

129. Paul Wallich, "Cyber View: Cracking the U.S. Code," Scientific American, April 1997, p. 42.

130. Declan McCullagh, "Fortification," Netly News, February 26, 1998. A contest among programmers to see who could turn on Netscape's strong encryption with the shortest program was won by a Russian programmer, who offered the following lines of Perl:

```
#!/usr/bin/perl-0777pi
s/(TS:.*?0)/$_=$1:y,a-z,,;s, $,true,gm;s,
512,2048,;$_/es;
```

Ibid.

131. Netscape was obliged to try to confirm whether requests to download the software provided names, addresses, and phone numbers and to affirm that requestors are U.S. citizens or green-card holders. "Netscape to Sell Advanced Encryption Software On-Line," Washington Post, July 16, 1996, p. C4.

132. Many observers believe that law enforcement is aware of and anxious to preserve this affect. Keyworth and Colton, p. 2 n.3.

133. NRC, p. 136.

134. NRC, p. 135.

135. NRC, p. 68.

136. NRC, p. 254.

137. The National Research Council concluded that the public debate about cryptography frames

> the policy issues as the privacy of individuals and businesses against the need of national security and law enforcement . . . this dichotomy is misleading. . . . If cryptography can . . . reduce economic espionage (which it can), it also supports . . . the job of law enforcement. If cryptography can help protect nationally critical information systems and networks . . . (which it can), it also supports the national security of the United States.

NRC, p. 3.

138. A report released by the Commerce Department found that many foreign-made encryption products are available overseas, and that in Switzerland, Denmark, and Britain, market share for encryption products made in the United States declined in 1994. Sources in 14 countries said that export controls limit U.S. market share, although those in 7 other countries reported little or no impact. Elizabeth Corcoran, "Encryption Rules Hurt Exporters, Study Says," Washington Post, January 17, 1996, p. A11.

139. James Barksdale, president and ceo, Netscape Communications Corporation, before the Senate Committee on Commerce, Science and Transportation, 25 July 1996, p. 8. See also offshore providers advertising at http://stronghold.ukweb.com and ftp://psy.uq.oz.au/pub/Crypto/SSL/README.

140. As of March 30, 1996, Trusted Information Systems, Inc. notes that "we have now identified 1181 products worldwide. . . . The survey results show that cryptography is indeed widespread throughout the world. . . . The quality of foreign products seems to be comparable to US products." Quoted in NRC, pp. 127-28.

141. Carol Bartz (Autodesk), Gregory Bentley (Bentley Systems), Bill Gates (Microsoft), Robert Fraukenberg (Novell), Lawrence Ellison (Oracle), Alok Mohan (Santa Cruz Operation), Mark Hoffman (Sybase), Gordon Eubanks (Symantec), Letter to Sen. Ted Stevens (R-Ark.) May 20, 1996, on file with author.

142. The Commerce Department report noted that in many of the countries surveyed, "exportable U.S. encryption products are perceived to be of an unsatisfactory quality." Corcoran, p. A11. The claim that foreign products are of inferior quality has been hotly contested; James Bidzos, for example, notes that foreign developers can simply study U.S. patents. James Bidzos, Statement before Subcommittee on Science, Technology, and Space of the Senate Committee on Commerce, Science, and Transportation, Hearing on S.1726, the Promotion of Commerce Online in the Digital Era Act of 1996, or "PRO-CODE," June 12, 1996, transcript, p. 61.

143. James Barksdale, Statement in ibid., pp. 5-6.

144. Brock Meeks, "Jacking in from the 'One That Got Away' Port," CyberWire Dispatch, June 3, 1996.

145. NRC, p. 134.

146. David Bank, "Sun's Selling of Encryption to Skirt Policy," Wall Street Journal, May 19, 1997, p. A3: and Tom Williams, "When Encryption Is Outlawed, Only Outlaws Will Encrypt," Electronic Design, September 2, 1997, p. 20.

147. See Bartz.

148. Under ITAR, items intended for the personal use of the exporter (such as programs stored on a laptop taken abroad to a business meeting) were exempt from export con-

trols. 15 C.F.R. Sec. 740.9 (1996). The new rules also allow such "temporary" exports.

149. "Published Source Code Raises New Encryption Questions," Computer and Communications Industry Association CEO Report, August 22, 1997, p. 2 (describing PGP, Inc.'s announcement that PGP 5.0 would be available for worldwide distribution in the form of published source code).

150. See http://www.ifi.uio.no/pgp/.

151. A complete description of DES, for example, is available worldwide. Froomkin, "The Metaphor Is the Key," pp. 736-37.

152. "All the FBI proposal would accomplish is to keep encryption out of the hands of U.S. companies and individuals concerned about their privacy rights, making them vulnerable to foreign espionage and criminal tampering and giving a huge advantage to foreign software companies selling encryption products in the U.S. market." Nathan P. Myhrvold, Testimony in Hearings on the Threat of Foreign Economic Espionage to U.S. Corporations, Subcommittee on Economical Commercial Law of the Committee on the Judiciary, HR102, 2nd Sess, Serial no. 65 (April 29 and May 7, 1997), p. 19. CCIA stated that "a voluntary key-recovery plan may be desirable and will work in certain circumstances. But we believe that forcing a key recovery or escrow system may still handcuff legitimate users of encryption technology, while 'true criminals and terrorists will not be compelled to adhere to a key-recovery system." CCIA Report, pp. 1-2.

153. NRC, p. 270. Steganography allows groups to conceal the content of a message without using encryption, which might attract the attention of the police. Free steganography software called S-Tools is available from a site in the United Kingdom. For an example of the use of steganography, see www.peoplink.org.

154. Freeh.

155. Clipper III Draft Proposal, p. 2.

156. Ibid., p. 2. The administration is "attempting to blur the line between a key certification system, where you confirm who you are by giving a public code to some kind of authority, like the Postal Service, and key escrow, which means giving the key to your program to a third party," said David Banisar . . . . "Commercial

transactions [over the Internet] may not be trustworthy without certification, but that problem has nothing to do with key escrow." Browning, p. 1955 (quoting David Banisar). "Data recovery--the ability to recover encrypted data if a private key is lost--is the main rationale presented for key escrow. However, data recovery can be done independently of the public key infrastructure if desired, and in a more secure manner. "Preliminary Analysis of 'Clipper III' Encryption Proposal," p. 3.

157. Gould, p. 5.

158. Freeh, p. 2.

159. Hal Abelson et al., The Risks of Key Recovery, Key Escrow, and Trust Third Party Encryption (Washington: Center for Democracy and Technology, May 1997), pp. 6-8, 9.

160. Clipper III Draft Proposal, p. 9.

161. Abelson et al., pp. 6-8, 9.

162. Ibid., p. 2.

163. Final letter from the National Institute of Standards and Technology Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure to the Honorable William M. Daley, June 19, 1998, http://www.cdt.org/crypto/letter2daley.html.

164. Will Rodger, "Technology Prolongs Crypto Impasse," Interactive Week, June 15, 1998, p. 58.

165. Gould, p. 5.

166. Barksdale, p. 14.

167. Private communications from George Spix to author, June 17, 1997.

168. William Reinsch, Memorandum for Deputies Subgroup on Cryptography, November 25, 1996, p. 1, http://www.epic.org/crypto/key_escrow/reinsch_memo_txt.html.

169. National Security Agency, "Threat and Vulnerability Model for Key Recovery (KR)," February 2, 1998, http://www.fcw.com/pubs/fcw/1998/0413/web-nsa report-4-14-1998.html.

170. Browning, p. 1954.

171. Diffie and Landau, p. 141.

172. See Frank J. Donner, The Age of Surveillance (New York: Alfred A. Knopf, 1980), pp. 244-48, 252-56, 276-77.

173. Froomkin, "The Metaphor Is the Key," pp. 731 n. 77, 733 n. 90; and Diffie and Landau, p. 138.

174. Burnham, p. 105; and Diffie and Landau, p. 144.

175. Tom Huston, a White House staffer under Nixon, said, "Covert [mail] coverage is illegal, and there are serious risks involved. . . . However, the advantages to be derived from its use outweigh the risks." Quoted in Diffie and Landau, p. 146. Then Attorney General Nicholas Katzenbach said that, although warrantless wiretaps are useless as court evidence, "we feel that the intelligence and the preventative aspect outweigh the desirability of prosecution in rare and exceptional circumstances." Quoted in ibid., p. 161. William Sullivan, then-director, Domestic Intelligence Division and assistant director, FBI, stated:

> We do not obtain authorization for "black bag" jobs from outside the Bureau [FBI]. Such a technique involves trespass and is clearly illegal; therefore, it would be impossible to obtain any legal sanction for it. Despite this, "black bag" jobs have been used because they represent an invaluable technique in combating subversive activities of a clandestine nature aimed directly at undermining and destroying our nation.

Memorandum to Cartha DeLoach, July 19, 1966, in The Macmillan Dictionary of Political Quotations, ed. Lewis D. Eigen and Jonathan P. Siegel (New York: Macmillan, 1993), p. 346.

176. NRC, pp. 32-33 (discussing threats from foreign agencies, such as the French intelligence agencies, plans to spy on U.S. business); Louis J. Freeh, "Address at the Executives' Club of Chicago, February 17, 1994, p. 8 (reporting that the governments of at least 20 nations are engaged in economic espionage); Froomkin, "The Metaphor Is the Key," p. 723 n. 43; and Diffie and Landau, p. 43.

177. Bill Gertz, "Foreign Spies Look to Acquire U.S. Economic and Trade Data," Washington Times, August 14, 1997, p. A6.

178. As of this writing, two of these bills have dropped out of the legislative picture. These include S. 377, entitled Promotion of Commerce Online in the Digital Era (PRO-CODE) Act of 1997, sponsored by Sen. Conrad Burns (R-Mont.). This bill would prohibit mandatory key escrow, and stipulates that the export of publicly available software or hardware under a general license shall be permitted, unless there is "substantial evidence" that the technology will be used for military or terrorist purposes, be reexported without authorization, or be "intentionally used to evade enforcement of United States law or taxation." The bill would also create an "Information Security Board" to help in formulating encryption policy. S. 376, the Encrypted Communications Privacy Act of 1997, introduced by Sen. Patrick Leahy (D-Vt.). This bill would ensure that it would be lawful to use encryption of any key length, and also outlaws mandatory key recovery. It also describes the circumstances under which a key holder (with whom a key has been voluntarily escrowed) may release a key to law enforcement. It would also instruct the Department of Commerce to allow the export of "generally available" encryption software (and hardware generally), with exceptions like S. 377. See Congressional Record, Senate, February 27, 1997, S1750-S59.

179. This bill would also legalize the use of any encryption technique and prohibit mandatory key escrow. The bill would also outlaw the use of encryption in "furtherance" of a criminal act. It would permit the export of "generally available" software, software in the public domain, or hardware, with exceptions similar to S. 377. Congressional Record, February 12, 1997, E246-E47 (statement of Rep. Bob Goodlatte).

180. Justin Matlick, "U.S. Encryption Policy: A Free-Market Primer," San Francisco: Pacific Research Institute for Public Policy, March 1998.

181. For the text of S. 6027, see http://www.cdt.org/legislation/text_S.6027.html.

182. Gore, "Statement of the Vice President," p. 1.

183. Clipper III Draft Proposal, p. 5.

184. Ibid., p. 9.

185. See also Abelson et al., pp. 9-11.

186. Browning, p. 1955 (quoting William A. Reinshch, commerce undersecretary for export administration). A spokesman for the Commerce Department has argued that "over time, the industry will have to get together and develop systems that permit [data authentication] to take place. So we're trying to devise a key escrow system that will fit into a lot of what we think will happen anyway."

187. Will Rodger, "South Africa's Thawte Adds Do-It-Yourself Crypto," Interactive Week, June 22, 1998, p. 48; and Eric Hammond, "Red Hat Offers Inexpensive, Trustworthy Web Solution," InfoWorld, July 6, 1998, p. 58.

188. Trevor v. Wood, 36 N.Y. 307 (1867); Howley v. Whipple, 48 N.H. 487 (1869); La Mar Hosiery Mills, Inc. v. Credit & Commodity Corp., 216 N.Y.S.2d 186 (1961)(deeming "[t]he telegram with the typed signature of defendant's name [to have] emanated from the defendant which is responsible for it.").

189. Selma Sav. Bank v. Webster County Bank, 206 S.W. 870, 874 (Ky. 1918) (contract is formed when message is transmitted to telegraph operator by telephone).

190. A telex is a communication system consisting of teletypewriters connected to a telephonic network that sends and receives signals. Teletypewriters are electromechanical typewriters that transmit or receive messages coded in electrical signals carried by telephone or telegraph wires. See Apex Oil Co. v. Vanguard Oil & Service Co., 760 F.2d 417 (2d Cir. 1985) (telex); Joseph Denuzio Fruit Co. v. Crane, 79 F. Supp. 117 (S.D. Cal. 1948), vacated, 89 F. Supp. 962 (S.D. Cal. 1950), reinstated, 188 F.2d 569 (9th Cir.), cert. denied, 342 U.S. 820 (1951); and Klein v. PepsiCo, Inc., 845 F.2d 76 (4th Cir. 1988).

191. Hessenthaler v. Farzin, 564 A.2d 990 (Pa. Super. 1989); Bazak Intl. Corp. v. Mast Industries, 535 N.E.2d 633 (N.Y. 1989); and Beatty v. First Exploration Fund 1987 & Co., 25 B.C.L.R.2d 377 (1988).

192. Beatty v. First Exploration Fund 1987 & Co., 25 B.C.L.R.2d 377 (1988) (comparing telefacsimiles and photocopies).

193. A tape recording of an oral agreement satisfies the writing requirement of the statute of frauds, since it has been reduced to tangible form. Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212, 1228 (D. Colo. 1972). See also Londono v. Gainsville, 768 F.2d 1223, 1227-28 n.4 (11th Cir. 1985). Another court, however, found that a

tape will not do, absent evidence that both parties intended to authenticate the record. Swink & Co. v. Carroll McEntee & McGinley, Inc., 584 S.W.2d 393 (Ark. 1979)

194. Howley v. Whipple, 48 N.H. 487, 488 (1869).

195. See for a copy of the act, which was passed by voice vote by the Senate Commerce, Science, and Transportation Committee. “Senate Oks Digital Signature, R&D Funding Bills,” Telecommunications Reports, August 3, 1998, p. 20.

196. Fredrick Seaton Siebert, Freedom of the Press in England 1476-1776 (Urbana: University of Illinois Press, 1952) p. 44.

197. Ibid., p. 31.

198. Ibid., p. 44.

199. Ibid., p. 31.

200. Ibid., p. 48.

201. Jonathan W. Emord, Freedom, Technology and the First Amendment (San Francisco: Pacific Research Institute for Public Policy, 1991), p. 27.

202. Ibid., p. 28, quoting Trenchard and Gordon, Cato's Letters.

203. Peter W. Huber, Orwell's Revenge (New York: Free Press, 1994).

204. Freeh, p. 4.

205. One noted failure involved FBI surveillance of rogue police officers. The FBI was unable to decode the police chief's "street slang and police jargon in time to foil a plot to murder someone who had filed a brutality complaint against the chief. NRC, p. 89 n. 11.

206. Ivan Eland, "Protecting the Homeland: The Best Defense Is to Give No Offense," Cato Institute Policy Analsys no. 306, May 5, 1998.

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before congress. Contact the Cato Institute for reprint permission. Additional copies of Policy Analysis are $6.00 each ($3.00 each for five or more). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Ave., N.W., Washington, D.C. 20001 or call toll free 1-800-767-1241 (noon - 9 p.m. eastern time) or fax (202) 842-3490 or visit our website at www.cato.org.