# Case Study of H.R. 695: The Security and Freedom Through Encryption (SAFE) Act

Catherine Miller Horiuchi

University of Southern California
Sacramento Municipal Utility District

Summer 1997; Revised, Summer 1998

"Denying millions of law-abiding people the use of a legitimate and increasingly necessary security product for 'law enforcement' reasons is like banning deadbolt locks because they make it a little harder to kick down the doors of a few drug dealers."

U.S Senator Conrad Burns[1]

The gangster Al Capone was convicted not for gun-running, bootlegging, murder or mayhem, but for tax evasion. As anyone who has seen the movie *The Untouchables* might remember, the star witness in this real-life drama was the bookkeeper, without whose testimony Capone might have remained a free man, despite the government's possession of the gangster's books. The bookkeeper had encoded entries, and his verification of the crudely encrypted transactions provided the basis for Al Capone's conviction.

Law enforcement needs information. Information and its encryption fuel law enforcement and military operations. In times of war and peace criminals and military foes have used cryptography to prevent access to privileged information, resulting in a long-standing administrative interest in cryptography. The National Security Council has one of the most advanced cryptography groups in the world. Navaho cryptographers helped the U.S. protect its miliary plans in World War II.

The private citizen needs privacy and protection of personal property. The Fourth Amendment to the U.S. Constitution states this need and the right for this privacy and protection.

This paper reviews the history of encryption policy, and analyzes the course of actions taken by the President, Congress, business and public interests, and various bureaucratic entities toward an updated, coherent policy on the encryption issue through the medium of H.R. 695. A summary assessment of the present situation and likely results are offered.

**Statement of Issue**

Technology at the turn of the millennium emulates the state of atomic energy fifty years ago. At the end of the war, following the destruction of Hiroshima and Nagasaki, attention turned to the peaceful application of atomic energy. The ability to split the atom was viewed as the bane of civilization, but potentially a boon as well. Nuclear power is the most pervasive and lasting example of peacetime use. Ironically, the U.S. is the one country least at peace about the role and residue of atomic energy.

In similar fashion, the application of technology is considered a potential silver bullet, a leveler of the playing field through providing seemingly limitless power, space, and access to the person sitting at the keyboard. The present administration, and Vice President Al Gore most particularly, has agressively pursued a technology leadership role for the U.S. in the global marketplace, and has mandated widespread use of computer technology in a vast arena of federally managed programs.

The technical progress in electronic communications, both voice and data, has expanded broadly the ability to transact legal and illegal business through electronic means. Legal business uses involving encryption include private messaging, secure transactions, database security, and source authentication. Criminal uses include preventing detection and obscuring evidence. These contradictory uses have resulted in the administration's desire to manage this technology. "The United States and other national governments have sought to prevent widespread use of cryptography unless 'key recovery' mechanisms guaranteeing law enforcement access to plaintext are built into these systems. The requirements imposed by such government-driven key recovery systems are different from the features sought by encryption users, and ultimately impose substantial new risks and costs." [2] Because many aspects of

legitimate business and personal interests are private and confidential, encryption is the standard method to ensure privacy across an inherently insecure public network.

The unique identifiers used in encryption and unencryption are called “keys”. There are several methods of encryption; most popular and widely discussed is the “pubic key / private key” algorithm. The sender encodes using the recipient’s public key; the recipient decodes using his or her own private key. This method is also used to authenticate the sender of the message, and the integrity of the transaction, in addition to preventing unwanted viewing of the message. The ability to break the key is inversely proportional to its length. The concept known as “key escrow” signifies the storage of keys to allow authorized access to any material that has been encoded. Some organizations have policy in place for corporate-wide key escrow, but this is a newly emerging area of technology management. Controversy arises over third-party or governmental key escrow. Encryption is required because the wires comprising our telecommunications and data networks are inherently insecure; wire-level security would require physical management and prevention from tampering along the full distance and at all switchpoints connecting two messaging points.

At the root of the legislative issue are two matters. One is a long-standing conflict between the government’s right to pursue criminals versus the citizens’ Fourth Amendment’s right “to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures”. As discussed historically, the government bears responsibility that “no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” Beyond any mistrust of warrants issued without probable cause comes the more serious matter of administration of key escrow, and protection from improper or unauthorized use. The second source of the legislative action derives from the Constitutional division of powers between the executive and legislative branches. Nearly all the federal rules governing encryption have been developed by various administrative agencies. Many businesses, academics, and private individuals are dissatisfied with the administrative policies, which are preponderantly focused on the needs of law enforcement, not on the rights of citizens and business interests. An onerous level of paperwork and bureaucratic management are imposed on buyers and sellers, reducing the robustness of the market.

The usage of encryption in illegal activities has resulted in law enforcement being hampered in its legal attempts to gather information on criminal activity, and to assemble evidence for use in trial proceedings. Encryption is essential, however, for growth in legal business activity using the communications infrastructure. Secure transactions through the Internet have expanded and enhanced the ability of small businesses to present their product in the marketplace, without having to directly compete and pay for shelf space in stores or floor space in shopping malls. For these small businesses, encryption allows commerce and expansion with broad ability to sell and limited risk of loss of revenue, as electronic commerce is based on familiar and well-established credit card transactions.

The companies who develop encryption technology for use in electronic commerce or private communications have been limited in the product allowed to be sold outside the U.S. This hampers their ability to compete in the global market and increases their operational expenses as they must develop, maintain, and monitor the sales of products for domestic use versus exports. The market for this software, worldwide, is not trivial. Stammberger, of RSA Data Security Inc., has pointed out that “The market is enormous, literally in the hundreds of

billions of dollars."[3] The dollars for encryption products will be spent, either on domestic products, or on those developed overseas.

Administrative efforts to satisfy governmental entities and industry have not succeeded, resulting in the industry leaders turning to Congress for legislative assistance and relief.

H.R. 695, the S.A.F.E Act, was designed to handle some of these issues. In the actual meandering of the bill through its various congressional stops, the markup process and multiple committee review is offering opportunity for revision and enhancement.

The Clinton Administration has had a differing agenda and approach, as seen in E.O. 13026, "Administration Of Export Controls On Encryption Products," signed November 15, 1996. Administrative actions since then have reiterated this basic stance. Issues continue to become more publicized, and it may be possible to have this act, or similar legislation, enacted by the present Congress.

Following sections detail activities from the origins of the issue to the current state within the 105th Congressional Session:.

**Historical Entities and Antecedents to H.R. 695**

1968 - Omnibus Crime Act authorized the FBI to wiretap telephones and eavesdrop on suspect activity. This is often cited as stating the government's right to examine any and all traffic, as warranted.

1991 - Phil Zimmerman releases his product, PGP, an abbreviation for "Pretty Good Privacy," the first widely distributed public/private key product. The original PGP was "freeware", distributed at no cost. Its original users were technically sophisticated and knowledgeable of the inherently insecure nature of wide area network traffic. Most encrypted and thus privatized and provided authentication for their personal electronic mail. Initially the government investigated Zimmerman, but ultimately he was not prosecuted. PGP, Inc. was actively involved in developing encryption policy. In late 1997, PGP was acquired by Network Associates.

1992 - The Clinton administration advocates development of the Clipper chip, a requirement for every computer to use this chip allowing the government access to everything on the computer. This concept was floated and sunk.

1993 - Marc Andreessen develops the Mosaic browser for X-windows, released through the National Center for Supercomputing Applications, and transforms the Internet by removing technological complexity, making the materials stored on Internet-connected systems accessible to the general public. The browser simplifies e-mail and the finding of materials of personal interest stored on sites throughout the world. This is the birth of the World Wide Web as the public understands it, and is the starting point of net "surfing."

1995 - Security experts unencrypt standard, exportable, Netscape encryption in 25 seconds. Thus, current allowable product is no longer acceptable for business and electronic commerce. Netscape posts a fix for the version on the Internet. This continues the cycle of point-counterpoint activities between developers and users of encryption against those who pursue decryption of others' traffic. "Hackers" -- one recognized term for

persons with this area of technical interest and focus -- enters the vernacular.

1995 - Louis Freeh, director of the FBI, speaks at a symposium sponsored by the International Cryptography Institute. He suggests a need for "a cop on the information superhighway," and argues that government ability to decrypt communications and files is "a public safety issue."

1996 - Executive Order 13026, "Administration of Export Controls on Encryption Products" is signed by Clinton, removing munitions status from encryption. It commits manufacturers to provide government with the means to unencrypt messages ("key escrow") created with over 40-bit encryption keys. Although many references consider this a voluntary key escrow system, tying the creatioin of a product to implementing key escrow is understood as tantamount to setting up a mandatory system.

**Bureaucratic Oversight - the Players**

OTA - Office of Technology Assessment - E.O. 13026 explicitly states that encryption software is not technology, but is subject to special controls, due to its functionality. Because of this odd classification, OTA appears one of the few administrative agencies not visibly engaged in the discussion of encryption.

BXA - Bureau of Export Administration - A sub-agency of the Commerce Department, th BXA is a principal player in encryption technology rulemaking, especially early on. This organization developed the Interim Rule among other actions that may have triggered a legislative response.

Commerce Department - Presently included in chain of organizations reviewing requests for export. Authorizes level of exportable encryption. Per E.O. 13026, "the Secretary of Commerce ('Secretary') may, in his discretion, consider the foreign availability of comparable encryption products in determining whether to issue a license in a particular case or to remove controls on particular products". In short, encryption software is not exportable unless overseas competitors already sell such software. At his discretion, the Secretary of Commerce may allow a company to sell a particular product; this is a discretionary decision, not a requirement. If a decision is made to allow exportation, the decision can be reviewed by the departments of State, Defense, Energy, and Justice, as well as the Arms Control and Disarmament Agency.

Department of Justice - DOJ reviews export license applications. As a law enforcement agency, DOJ is especially interested in forcing key escrow, or what is now referred to as the key recovery infrastructure. The KRA, Key Recovery Alliance, is a technology companies umbrella group attempting to develop key recovery. After acquiring PGP, Network Associates drops out of the KRA.

FBI - the Federal Bureau of Investigations - Congressional action legalized wiretapping in the Omnibus Crime Act in 1968. This act is often referenced by regulatory proponents in encryption and Fourth Amendment rights discussion, with the interpretation that criminals' rights are limited, or, as Director of the FBI Louis J Freeh has remarked, "criminals do not have the right to privacy with respect to the planning and commission of crimes"[4]. Per this analysis, the same law enforcement warranted ability to wiretap extends to its right to unencrypt information as part of normal investigations. As a law

enforcement agency, the FBI is interested in the development of the key recovery infrastructure. As Louis J. Freeh has said, "We need access to the records that grand juries have been able to see for hundreds of years and which the courts of this country have allowed us to get." [5]

NIST - National Institute of Standards and Technology - In response to the Administration's "key management infrastructure" initiative, NIST has set up a committee to develop standards and requirements. These meetings are also attended by representatives of foreign governments.[6] David Aaron, ambassador to the Organization for Economic Cooperation and Development (OECD), and now designated U.S. special envoy for encryption policy, represents the U.S. in the meetings.

**Actions by the General Populace and Non-Governmental Organizations**

A January 1997 article in the online version of the Washington Post[7] included a link to an Internet site where the user could, by clicking on a button, cause an encryption program to be sent to a computer outside the United States. Until November of 1996, this act would have transformed the user into an "International Arms Dealer," since encryption programs were classified as munitions. The page was set up in 1996 as a forum and a source method for civil disobedience; it included the option for each participant to also send e-mail to the White House, informing the government of the action taken.[8]

A number of standing and newly formed coalitions constitute the non-governmental community of interest supporting this bill. Their membership includes most members of the Internet Privacy Coalition, the American Civil Liberties Union (ACLU), the Electronic Privacy Information Center, the Center for Democracy and Technology, and the U.S. Association for Computing Machinery (USACM), through its Public Policy Committee.

**Administrative Action**

President Clinton has acted on encryption as an issue of "national security." The administration has the authority to act independently from Congress in such matters; the executive order cited above was one result.

Signed November 15, 1996, E.O. 13026 redefines encryption as neither technology nor munitions, and establishes bureaucratic review for product exportation:

> "This order is intended only to improve the internal management of the executive branch and to ensure the implementation of appropriate controls on the export and foreign dissemination of encryption products. It is not intended to, and does not, create any rights to administrative or judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person."[9]

Despite the Administration's active support for the development of a key management infrastructure and its stated opposition to HR 695, the President himself has concerns on the issue of protecting the privacy of individuals. He gave the 1997 commencement address at Morgan State University, where he made the following remarks:

> "[T]echnology should not be used to break down the wall of privacy and autonomy free citizens are guaranteed in a free society. The right to privacy is one of our most cherished freedoms. As society has grown more complex and people have become more interconnected in every way, we have had to work even harder to respect the privacy ... of each individual.... As the Internet reaches to touch every business and every household and we face the frightening prospect that private information -- even medical records -- could be made instantly available to the world, we must develop new protections for privacy in the face of new technological reality."[10]

Clinton's recognition that privacy issues are a principal concern suggests the possibility of positional compromise between the Administration's activities on encryption control and the content of H.R. 695.

Another sign of progress in bringing the two sides together appeared in the May 17, 1997 issue of Congressional Quarterly:

> "Even though the White House has expressed opposition to the export provisions in the bill, administration officials met the week of May 12 with Goodlatte and Judiciary Committee Chair Henry J. Hyde, R-Ill, as part of an effort to work out a compromise."

Two days later, the Judiciary Committee released the bill favorably.

Hearings in early June 1997 by the Federal Trade Commission (FTC) demonstrated public concerns on the issue of Internet privacy. These hearings were triggered by fears about the collection of user information by web sites. Two types of information collection have raised concerns: the collection and later utilization of information submitted by children on user forms, and the collection and later utilization of information without knowledge or approval of users ("cookies" is the term used, and the file created by this process is called cookies.txt). This information is re-marketed for profit, as well as used by companies' internal marketing groups. Sophisticated users may encrypt messages, post to online forums with invalid e-mail return addresses (my_BOGUS_email_id@company.com,) and use strong security on their personal computers to protect their confidentiality. The ability for more typical computer users to better protect themselves is being built into some operating systems, browsers and email packages.

## Congressional Action and Review

A step back is required to review the course of action from the legislative point of view.

Representative Robert W. Goodlatte introduced H.R. 3011 in the 104th Congress. The Committee on International Relations held a single day of hearings on the bill, but no additional action was taken in the 104th Congress.

On February 12, 1997, Representative Robert W. Goodlatte (Republican, Virginia) introduced H.R. 695, identical in language to H.R. 3011: "a bill to amend title 18, United States Code, to affirm the rights of U.S. persons to use and sell encryption of and to relax export controls on encryption," which differs materially from the Administration's policy by allowing the use of all forms of encryption and prohibiting any mandatory encryption key management. (Full text of H.R. 695 is found in Appendix A.)

On February 12, 1997, that same day, the bill was referred to the Committee on the Judiciary, and in addition to the Committee on International Relations. Also on that date, the

U.S. Public Policy Committee for the Association for Computing Machinery (USACM) sent a letter to the BXA on their concerns about the Interim Rule to develop the Key Recovery Infrastructure.

The bill was introduced with 54 co-sponsors, one of whom subsequently withdrew sponsorship. Since its introduction, an additional 69 members became co-sponsors, one of whom subsequently withdrew. One of these persons, Representative Gerald B. Solomon, wrote a "Dear Colleague" letter expressing his concerns. That letter aside, the growing support of 122 cosponsors suggested the bill was gathering steam. Since 218 members are needed to pass a bill, this measure needed less than one additional member per sponsor to vote in favor of the bill for it to move forward, out of the House and into the Senate. Or, cutting the numbers another way, imagining a floor vote could split 50-50 among the 313 members, these 156 votes would push the measure over the top with a sixty-member margin.

On March 3, 1997, the bill was referred to the Subcommittee on International Economic Policy and Trade.

On March 5, 1997, it was referred to the Subcommittee on Courts and Intellectual Property. The first hearing on the bill by the Subcommittee on Courts and Intellectual Property was held on March 20.

On April 28, 1997 the Internet Privacy Coalition sent a letter to the Judiciary Committee in support of H.R. 695. This coalition is an example of the adage, "politics make strange bedfellows" – its members range from the American Civil Liberties Union, through the USACM, several electronic commerce software vendors, and the conservative Eagle Forum. The letter requested removal of the provision creating additional criminal penalties, if a crime is furthered through the use of encryption:

> "Such a provision tends to draw attention away from the underlying criminal act and casts a shadow over a valuable technology that should not be criminalized. It may, for instance, be the case that a typewritten ransom note poses a more difficult challenge for forensic investigators than a handwritten note. But it would be a mistake to criminalize the use of a typewriter simply because it could make it more difficult to investigate a crime in some circumstances."[11]

On April 30, 1997, the Subcommittee Consideration and Mark-up Session was held. The same day, the full Committee made its selection by voice vote.

At a May 8, 1997 open meeting of the International Relations Subcommittee on International Economic Policy and Trade, Bureau of Export Administration Under Secretary William Reinsch testified on the Administration's behalf. He stated the Administration's actions and objectives, and stressed his opposition to HR 695. In response to his testimony, "Many of the Committee members were adamant in their opposition to Administration policy on this issue."[12]

On May 14, 1997, the House Judiciary Committee approved the bill. After full committee consideration and mark-up, the Committee recommended the bill be reported as amended, by voice vote. The amendment involved removing any emphasis suggesting that encryption is inherently criminal in nature.

On May 22, 1997, the amended bill was reported to the House Committee on Judiciary.

Prior to the Fourth of July recess, the bill remained in the International Relations Committee. That committee had twenty-three majority (Republican) members and twenty-two minority (Democrat) members. Neither the committee chairman, Representative Benjamin Gilman of New York, nor the ranking minority member, Representative Lee Hamilton of Indiana, was a co-sponsor of the bill. Of the 122 sponsors, however, twenty-two were on this committee. Of those twenty-two, eleven were Republicans, eleven Democrats. This showed the bipartisan support for the bill that suggested it would likely move forward. A staff member from Representative Edward Royce's office expected the bill to appear on the House floor after the Fourth of July recess.

**Next Steps & Possible Outcomes**

The Rules Committee could make a rule to limit debate, or to pass by voice vote only. This could allow the bipartisan support for the measure to quickly gain passage, without having a vote of record. No Congressman is especially pleased to have to choose between supporting his party's President and supporting business growth on the Internet and private citizens' right to privacy. A voice vote would allow a Democrat to support the bill without being on record as acting in contradiction to the administration's position. Limited debate lets a handful of supporters stand up and talk about the value of the bill for American competitiveness, the respect for personal privacy that encryption allows, and brings House closure on the issue while the public's attention rests on the impropriety of surreptitious collection and viewing of personal information possible on the Internet.

On the Senate side, no similar measure was currently passing through the Senate. But Senator Bob Kerrey, Democrat, Nebraska, was drafting legislation to create, in his terms, "a secure public network". Given the mixed public statements of the Administration to date, it seemed possible H.R. 695 could pass through the House and Senate, only to be vetoed by the President. At the time, Administration remarks on the privacy issues, and conciliatory comments began to appear, suggesting potential for compromise, especially if the reputed Kerrey bill included details on the instances allowing law enforcement to seek the release of keys.

Given a national goal of leading in technology development, it is not surprising that U.S. developed encryption has world-class functionality. The ever-increasing ability to search for any information stored on any Internet-attached network -- including automated searches through "webcrawler" agents -- is resulting in more business and private information becoming encrypted.

The bureaucratic forces that have given the American people the Internal Revenue Service are not broadly respected. Publicity about IRS workers circulating the returns of celebrities demonstrates the validity of concerns about the government's ability to manage confidential information on hundreds of millions of persons. It is not likely that any governmental prerogative for key escrow will find broad support among citizens, business, or the legislators who represent their interests.

Lacking consensus between the legislative and executive branches, an acceptable overall policy will be difficult to develop. Evidence that this is recognized comes in the splitting off of various functional aspects of encryption. Attempts are being made to separate the exportation of encryption from the use of encryption in financial transactions and the use of encryption to

protect the confidentiality of certain correspondence or personal records.

The administration continues to pursue a strategy for a key management infrastructure, with voluntary compliance. A team of highly regarded security experts, in their May 27, 1997 paper, state that this concept may not be possible.

> "The deployment of key-recovery-based encryption infrastructures to meet law enforcement's stated specifications will result in substantial sacrifices in security and greatly increased costs to the end-user. Building the secure computer-communication infrastructures necessary to provide adequate technological underpinnings demanded by these requirements would be enormously complex and is far beyond the experience and current competency of the field. Even if such infrastructures could be built, the risks and costs of such an operating environment may ultimately prove unacceptable. In addition, these infrastructures would generally require extraordinary levels of human trustworthiness. "[13]

Undersecretary Reinsch concurs with this opinion; in his May 8, 1997 testimony he stated that the administration's key recover concept requires "a range of technologies, some in existence, some under development, some still being conceived, designed to permit the plaintext recovery of encrypted data or communications."

Technological hurdles aside, there is still the question of securing these technologies, and assuring they are only used in legal processes, as defined within the Fourth Amendment to the Constitution. The question is raised by Abelson et al. regarding the "extraordinary levels of human trustworthiness" required.

Companies producing this technology find the rules and regulations are unstable and change regularly. This affects their business planning and may discourage overseas business. Where they must compete with companies facing no such limitations, some software vendors are adapting and making plans, in concord with the current policy. These efforts include acquisition of foreign providers of strong encryption, relocation of some operations outside the U.S., or special permissions from the Administration to provide operating systems or software holes into which strong encryption can be embedded by buyers. Some companies now write their Congressmen and are beginning to appear at governmental public hearings. From Undersecretary Reinsch's May 8th remarks:

> "We asked for public comments on this new regulation. We received 43. They are posted on BXA's web site for all to review. Some are critical, but many are very helpful. Perhaps a better gauge of industry response has been the flow of applications since the change in policy. In the first two months we have received close to 700 license applications for exports valued at almost $800 million. Twenty four companies have submitted commitment plans which lay out how they will build and market key recovery products, and we know that others are preparing them. These companies include some of the largest software and hardware manufacturers in the country. We have approved twelve of these plans, and we expect to approve more very shortly. None have been rejected."

The above statement was not borne out by other sources, including some participating companies.

PGP, Inc., a major exporter of encryption technology, on the PGP Web Site

www.pgp.com presented an overview of their government agreement to export encryption software. From their online newsroom press release come the good news, "Pretty Good Privacy, Inc. has recently announced that it has obtained an export license from the U.S. government permitting PGP to ship its mail encryption products (full strength and without key recovery!)"[14]

The following anecdote from a 1997 security conference appeared in Inter@ctive Week, an online periodical:

> "Federal officials and privacy advocates argued bitterly... David Aaron, U.S. special envoy for encryption policy, told participants... that encryption markets worldwide will soon include -- if not be dominated by -- so-called key recovery or key escrow technologies now being promoted by the federal government... But only hours later, a prominent privacy advocate tore up a previously prepared presentation and instead blasted the Clinton administration envoy.... Marc Rotenberg, director of the Electronic Privacy Information Center in Washington, D.C., said the OECD meetings had, in fact, strongly distanced themselves from the U.S. position on key escrow. 'There is no -- and I repeat no -- international consensus within the OECD for lawful access to encryption data', Rotenberg said."

**Summation**

Development of the electronic commerce industry results in an enlargement of the marketplace, and creates opportunity for small businesses to start up and prosper. Their need to transact secure business, domestically and overseas, is a principal driver in changing the definition of encryption, and expanding its usability. These groups require the use of the strongest encryption available; they are not interested in a bureaucratic process that slowly ratchets the allowable encryption up, much more slowly than better encryption is developed and weaker encryption is breached. Regardless of the fate of H.R. 695, financial institutions may be able to establish trusted third-party key escrow within the limits of the current restrictions. Possible results from this Congress's work on H.R. 695 include death in committee or on the floor, presidential veto, passage and enactment with minor amendment, passage and enactment with major amendment, or the development of additional legislation to more fully address the needs of law enforcement. From an early vantage point, passage with amendment combined with additional special legislation seemed most likely.

Looking forward, these same issues, perhap worse, can be expected with the development of the digital signature and biometrics. Technologies to establish secure signature and authentication are emerging. Once agreed-upon standards are established, it is likely that security-oriented governmental agencies will want the ability to override these as well. Instead of broad legislation addressing this in conjunction with encryption and privacy issues, more likely numerous discrete rules will be developed, narrowly managing portions of the overall picture. Individual regulation tends to overlap and be contradictory, but it is much easier to enact and implement.

Keeping up with the rate of technology change is no simple matter for the average citizen. For a slow, deliberative, process-oriented entity like Congress, keeping up is outside the realm of possibility. Technology developers today have intensity, focus, and rigor similar to researchers seeking post-war peacetime use of atomic power. The workweeks of millions are filled with new inventions, market shifts and exploitation, threats and counterthreats to

business intelligence. A particular technology can rise to dominance and fall to bankruptcy within the span of a single Congress.

Given this difficulty, a new process for determining necessary review is required; development of a national technology vision and government's role in fulfilling the vision is a better approach for government to follow. The legislature needs to take initiative, to limit the opportunity and necessity for the executive branch and the federal bureaucracy to take action with little public representation. An absence of legislative discussion and process upsets the Constitutional balance of powers and causes difficulties for individuals and businesses attempting to cooperate with the government while pursuing personal goals. Responding to the challenge that the technical rate of change poses could be a catalyst to further streamline bureaucratic agencies and management processes.

The Clinton Administration has been active in promoting its vision of our technological future. Congress's Constitutional responsibility to provide representation of constituents' concerns, and balance to the executive branch, requires it to reflect deeply on technology issues and provide suitable legislative support.

Technology interests have traditionally shied away from government, focusing on the work at hand of growing the business. At this point, the industry is beginning to understand that showing up at Congress is a means to achieve equity and balance, the equivalent of working with business partners at the bargaining table. Proper legislative support is essential to furthering the growth of technology to promote business and governmental interests. For all the above reasons, following the development of H.R. 695 is a civics lesson for the technology community, fostering the travels of an industry's interests through Congress to enactment.

**Postscript: What Happened to H.R. 695?**

Contrary to suggestions made earlier in this paper, H.R. 695 did not get through Congress in 1997. In the Senate, hearings were held and proposals made to require mandatory key escrow for all levels of encryptions, including encryption imported from outside the U.S. While the House International Relations Committee approved H.R. 695 on July 23, 1997, the Senate in July heard from Louis Freeh of the FBI on the requirements of law enforcement for "real-time decryption." As H.R. 695 moved on into the House National Security Committe, an amendment was added by Representatives Curt Weldon (R-PA) and Ron Dellums (D-CA) which removed the bill's reforms of export controls, returning export discretion to the Administration. Thereafter, on September 11 the House Intelligence Committee developed its own amendment, proposed by Porter Goss (R-FL) and Norman Dicks (D-WA) adding many encryption controls and banning all encryption products that could prevent law enforcement's "immediate access" to information within an encrypted message. The amendment which received the most attention was the Oxley/Manton Amendment, developed with input from the FBI; this was rejected by the House Commerce Committee September 24, 1997. Many felt the Oxley/Manton Amendment was unconstitutional, a violation of the Fourth Amendment, with its provision for immediate access without knowledge of the user, upon undefined judical process. House Rules Committee Chairman Gerald Solomon refused to bring the bill before the whole House without the Oxley-Manton amendment, so the bill did not advance.

The 1998 legislative session has seen introduction of several pieces of legislation; none appears to bring the opposing sides closer together. The Presidental Commission for Critical

Infrastructure Protection (PCCIP) has brought out the risks of information and infrastructural warfare. The risks and oppportunites in the interconnected realm may encourage the Administration to accede the value of strong encryption, and to develop policy that protects the Constitutional rights of the large mass of citizens who use encryption to reasonably ensure information on a network with high public access. Though the needs, complexity, and importance of these technologies grow, the challenge remains to simplify the number of agencies, to limit overlapping jurisdiction, and to support legitimate and constitutionally protected rights while providing defense and law enforcement adequate tools for this new domain.

**Bibliography**


Abelson, Hal, et al. "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption." http://www.crypto.com/key_study/report.shtml (May 1997)

"Analysis of Revised Oxley-Manton Amendment". http://www.cdt.org/crypto/legis_105/SAFE/OxlMan_rev_analysis.html 9/23/1997. (June 1998).

"Bill Summary & Status for the 105th Congress: H.R. 695." http://thomas.loc.gov/cgi-bin/bdquery/z?d105:h.r.695: (May 1997)

"House Judiciary Committee Approves SAFE Internet Privacy Bill." CDT Policy Post Volume 3, Number 4 14 May 1997. http://www.cdt.org/publications/pp_3.04.html (June 1997).

Chandrasekaran, Rajiv, "Software Firms Call U.S. Plan on Encryption 'Unworkable'." Washington Post 11 December 1996. http://www.washingtonpost.com/wp-srv/tech/analysis/encryption/unwork.htm (May 1997).

Davidson, Roger H. and Oleszek, Walter J. (1994). Congress and Its Members. Washington, CQ Press, 1994.

"Encryption for the Rest of Us." Washington Post http://www.washingtonpost.com/wp-srv/tech/analysis/encryption/encrypt.htm (May 1997).

Gruenwald, Juliana. "Panel Votes to Ease Rules on Encryption Exports", Congressional Quarterly 17 May 1997.

"H.R. 695 - The "SAFE" Bill - Latest News." ".http://www.cdt.org/crypto/legis_105/SAFE/latest.html (June 1998).

http://www.bxa.doc.gov/bxaissue.htm (May 1997).

http://www.bxa.doc.gov/eo13026.htm (May 1997).

http://www.epic.org/privacy/laws/clinton_speech_5_18_97.html#privacy (May 1997).

http://www.pgp.com/newsroom/prel34.cgi (May 1997).

http://www.washingtonpost.com/wp-srv/tech/analysis/encryption/40bit.htm (May 1997).

http://www.washingtonpost.com/wp-srv/tech/analysis/encryption/burns.htm (May 1997).

"ITAR Civil Disobedience (International Arms Trafficker Training Page)." http://online.offshore.com.ai/arms-trafficker (May 1997).

Johnson, Charles W. "How Our Laws Are Made", February 1997. http://thomas.loc.gov/home/lawsmade.toc.html (June 1997).

"KRA's Corrections to December 9, 1997 CyberTimes Extra Article." http://www.kra.org/clips/NYTDec11.html (June 1998)

"Network Associates Withdraws from Key Recovery Alliance." http://www.pgp.com/newsroom/na-kra.cgi. (December 1997)

Rodger, Will. "Consensus On International Encryption Policies Challenged." Inter@ctive Week 29 January 1997. http://www4.zdnet.com/intweek/daily/970129b.html (June 1997).

"Security and Freedom through Encryption Act: Report", ftp://ftp.loc.gov/pub/thomas/cp105/hr108pl.txt (June 1997).

Simons, Barbara. "USACM's Comments on Interim Regulations on Cryptography", 12 February 1997. http://info.acm.org/usacm/usacm_crypto_comments.html.

"Why Encryption is Necessary", htttp://www.pgp.com/privacy/necessary.cgi (June 1997).

**Appendix A**

HR 695 IH

105th CONGRESS
1st Session
H. R. 695

To amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption.

IN THE HOUSE OF REPRESENTATIVES

February 12, 1997

Mr. GOODLATTE (for himself, Ms. LOFGREN, Mr. DELAY, Mr. BOEHNER, Mr. COBLE, Mr. SENSENBRENNER, Mr. BONO, Mr. PEASE, Mr. CANNON, Mr. CONYERS, Mr. BOUCHER, Mr. GEKAS, Mr. SMITH of Texas, Mr. INGLIS of South Carolina, Mr. BRYANT, Mr. CHABOT, Mr. BARR of Georgia, Ms. JACKSON-LEE of Texas, Ms. WATERS, Mr. ACKERMAN, Mr. BAKER, Mr. BARTLETT of Maryland, Mr. CAMPBELL, Mr. CHAMBLISS, Mr. CUNNINGHAM, Mr. DAVIS of Virginia, Mr. DICKEY, Mr. DOOLITTLE, Mr. EHLERS, Mr. ENGEL, Ms. ESHOO, Mr. EVERETT, Mr. EWING, Mr. FARR of California, Mr. GEJDENSON, Mr. GILLMOR, Mr. GOODE, Ms. NORTON, Mr. HORN, Ms. EDDIE BERNICE JOHNSON of Texas, Mr. SAM JOHNSON of Texas, Mr. KOLBE, Mr. MCINTOSH, Mr. MCKEON, Mr. MANZULLO, Mr. MATSUI, Mr. MICA, Mr. MINGE, Mr. MOAKLEY, Mr. NETHERCUTT, Mr. PACKARD, Mr. SESSIONS, Mr. UPTON, Mr. WHITE, and Ms. WOOLSEY) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on Internaional Relations, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the `Security and Freedom Through Encryption (SAFE) Act'.

SEC. 2. SALE AND USE OF ENCRYPTION.

(a) IN GENERAL- Part I of title 18, United States Code, is amended by inserting after

chapter 121 the following new chapter:

`CHAPTER 122--ENCRYPTED WIRE AND ELECTRONIC INFORMATION



`Sec. 2801. Definitions

`As used in this chapter--

`(1) the terms `person', `State', `wire communication', `electronic communication', `investigative or law enforcement officer', `judge of competent jurisdiction', and `electronic storage' have the meanings given those terms in section 2510 of this title;

`(2) the terms `encrypt' and `encryption' refer to the scrambling of wire or electronic information using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such information;

`(3) the term `key' means the variable information used in a mathematical formula, code, or algorithm, or any component thereof, used to decrypt wire or electronic information that has been encrypted; and

`(4) the term `United States person' means--

`(A) any United States citizen;

`(B) any other person organized under the laws of any State, the District of Columbia, or any commonwealth, territory, or possession of the United States; and

`(C) any person organized under the laws of any foreign country who is owned or controlled by individuals or persons described in subparagraphs (A) and (B).

`Sec. 2802. Freedom to use encryption

`Subject to section 2805, it shall be lawful for any person within any State, and for any United
States person in a foreign country, to use any encryption, regardless of the encryption

algorithm selected, encryption key length chosen, or implementation technique or medium used.

`Sec. 2803. Freedom to sell encryption

`Subject to section 2805, it shall be lawful for any person within any State to sell in interstate commerce any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

`Sec. 2804. Prohibition on mandatory key escrow

`(a) PROHIBITION- No person in lawful possession of a key to encrypted information may be required by Federal or State law to relinquish to another person control of that key.

`(b) EXCEPTION FOR ACCESS FOR LAW ENFORCEMENT PURPOSES- Subsection (a) shall not affect the authority of any investigative or law enforcement officer, acting under any law in effect on the effective date of this chapter, to gain access to encrypted information.

`Sec. 2805. Unlawful use of encryption in furtherance of a criminal act

`Any person who willfully uses encryption in furtherance of the commission of a criminal offense for which the person may be prosecuted in a court of competent jurisdiction--

`(1) in the case of a first offense under this section, shall be imprisoned for not more than 5 years, or fined in the amount set forth in this title, or both; and

`(2) in the case of a second or subsequent offense under this section, shall be imprisoned for not more than 10 years, or fined in the amount set forth in this title, or both.'.

(b) CONFORMING AMENDMENT- The table of chapters for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 33 the following new item:

2801'.

SEC. 3. EXPORTS OF ENCRYPTION.

(a) AMENDMENT TO EXPORT ADMINISTRATION ACT OF 1979- Section 17 of the Export Administration Act of 1979 (50 U.S.C. App. 2416) is amended by adding at the end thereof the following new subsection:

`(g) COMPUTERS AND RELATED EQUIPMENT-

`(1) GENERAL RULE- Subject to paragraphs (2), (3), and (4), the Secretary shall

have exclusive authority to control exports of all computer hardware, software, and technology for information security (including encryption), except that which is specifically designed or modified for military use, including command, control, and intelligence applications.

`(2) ITEMS NOT REQUIRING LICENSES- No validated license may be required, except pursuant to the Trading With The Enemy Act or the International Emergency Economic Powers Act (but only to the extent that the authority of such Act is not exercised to extend controls imposed under this Act), for the export or reexport of--

`(A) any software, including software with encryption capabilities--

`(i) that is generally available, as is, and is designed for installation by the purchaser; or

`(ii) that is in the public domain for which copyright or other protection is not available under title 17, United States Code, or that is available to the public because it is generally accessible to the interested public in any form; or

`(B) any computing device solely because it incorporates or employs in any form software (including software with encryption capabilities) exempted from any requirement for a validated license under subparagraph (A).

`(3) SOFTWARE WITH ENCRYPTION CAPABILITIES- The Secretary shall authorize the export or reexport of software with encryption capabilities for nonmilitary end uses in any country to which exports of software of similar capability are permitted for use by financial institutions not controlled in fact by United States persons, unless there is substantial evidence that such software will be--

`(A) diverted to a military end use or an end use supporting international terrorism;

`(B) modified for military or terrorist end use; or

`(C) reexported without any authorization by the United States that may be required under this Act.

`(4) HARDWARE WITH ENCRYPTION CAPABILITIES- The Secretary shall authorize the export or reexport of computer hardware with encryption capabilities if the Secretary determines that a product offering comparable security is commercially available outside the United States from a foreign supplier, without effective restrictions.

`(5) DEFINITIONS- As used in this subsection--

`(A) the term `encryption' means the scrambling of wire or electronic information

using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such information;

`(B) the term `generally available' means, in the case of software (including software with encryption capabilities), software that is offered for sale, license, or transfer to any person without restriction, whether or not for consideration, including, but not limited to, over-the-counter retail sales, mail order transactions, phone order transactions, electronic distribution, or sale on approval;

`(C) the term `as is' means, in the case of software (including software with encryption capabilities), a software program that is not designed, developed, or tailored by the software publisher for specific purchasers, except that such purchasers may supply certain installation parameters needed by the software program to function properly with the purchaser's system and may customize the software program by choosing among options contained in the software program;

`(D) the term `is designed for installation by the purchaser' means, in the case of software (including software with encryption capabilities) that--

`(i) the software publisher intends for the purchaser (including any licensee or transferee), who may not be the actual program user, to install the software program on a computing device and has supplied the necessary instructions to do so, except that the publisher may also provide telephone help line services for software installation, electronic transmission, or basic operations; and

`(ii) the software program is designed for installation by the purchaser without further substantial support by the supplier;

`(E) the term `computing device' means a device which incorporates one or more microprocessor-based central processing units that can accept, store, process, or provide output of data; and

`(F) the term `computer hardware', when used in conjunction with information security, includes, but is not limited to, computer systems, equipment, application-specific assemblies, modules, and integrated circuits.'.

(b) CONTINUATION OF EXPORT ADMINISTRATION ACT- For purposes of carrying out the amendment made by subsection (a), the Export Administration Act of 1979 shall be deemed to be in effect.

**Endnotes**

---

[1] Burns, Conrad. “Speaking in Code on the Internet”, Washington Post, 8/9/1996, pg. A16

[2] Abelson et al. “The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption”, Section 1.2

[3] *http://www.washingtonpost.com/wp-srv/tech/analysis/encryption/40bit.htm* from the Associated Press, 1/29/97

[4] Speech by Louis J. Freeh, Director of the FBI , before the International Cryptography Institute, Washington, D.C., September 21, 1995. *http://www.fbi.gov/dirspch/crypto.htm*

[5] Ibid.

[6] From Undersecretary Reinsch’s May 8th testimony, *http://www.bxa.doc.gov/bxaissue.htm*

[7] Dan Pacheco and Michael Whitney “Encryption for the Rest of Us”

[8] This site is found at *http://online.offshore.com.ai/arms-trafficker/*. Checkboxes ask the participant,

“How public do you want your protest to be?

Don't tell anyone that I'm an arms trafficker

Add me to the public list of Known Arms Traffickers

Add me to the list and send a letter to the president for me”

[9] Executive Order 13026, November 15, 1996, Section 3. *http://www.bxa.doc.gov/eo13026.htm*

[10] White House press release, May 18, 1997. Available online at *http://www.epic.org/privacy/laws/clinton_speech_5_18_97.html#privacy*

[11] From the Internet Privacy Coalition Internet Site,

[12] From the Bureau of Export Administration’s Internet Site, *http://www.bxa.doc.gov/bxaissue.htm*

[13] Abelson, Hal, et al. “The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption” http://www.crypto.com/key_study/report.shtml

[14] This news breifing continues to explain some of the details of their BXA agreement, including the requirement to report “every six months the item description, quantity, value, and the enduser name and address of all transactions made under the export license”. “Export License for the Large U.S. Corporation” http://www.pgp.com/newsroom/export_lic.cgi.

# H.R. 695:  The S.A.F.E Act

Catherine Miller Horiuchi
University of Southern California
Sacramento Municipal Utility District
Summer 1997; revised Summer 1998

"Denying millions of law-abiding people the use of a legitimate and increasingly necessary security product for 'law enforcement' reasons is like banning deadbolt locks because they make it a little harder to kick down the doors of a few drug dealers."

U.S Senator Conrad Burns

# Origins of Issue

- Encryption usage
  - Legitimate
    - private messaging - electronic mail (e-mail), telephone
    - secure transactions
      - electronic banking
      - catalog sales, airline ticketing
    - database security
    - authentication
  - Criminal
    - prevent detection
    - obscure evidence

# How Encryption Works

- Several methods
- Most popular - public key/private key
- Send others public key, keep private key
- Use private key to encrypt
- Length of key determines likelihood of cracking

# Evolving Administrative View of Encryption Issue

- Munitions
- Not technology
- Impediment to criminal investigation. Needs to be removable by warranted government agents

# Bureaucratic Oversight

- OTA
- BXA
- Commerce
- DOJ
- NIST
- FBI

# External Support for H.R. 695

- Software Companies
- Computer Scientists/researchers
- Privacy Advocates
- General Business Advocates
- ACLU
- Financial Institutions

# Internal Opponents to H.R. 695

- FBI
- National Security Council
- Vice President, on behalf of Administration
- Bureaucracies currently controlling this technology

# Progress Toward Enactment - 1997

- No action taken in 104th Congress
- In 105th Congress, 122 bill sponsors
- Bi-partisan support (22 sponsors on House International Relations Committee, 11 each, Republican and Democrat)
- Oxley/Manton Amendment defeat
- Rules Committee -- version consolidation

# H.R.695 Possible Outcomes

- Special rules from Rule Committee to enhance, encourage support from Democratic members; or to stop measure
- Strong public support, specific administrative opposition
- Could go through Senate rapidly; or could face strong objection
- Amendments to prevent presidential veto

# Progress on Encryption Rules 1998

- New bills in House and Senate
- PCCIP
- Additional oversight and coordination agencies

# Fragmented Technology Policy

- Multiple agency oversight
- Separation of interlocking issues
- Political expediency
- Bureaucratic inertia
- Industry naivete on governmental operations
- Limited grassroot organizations