Global Information Assurance Certification Paper

Victorian F. Paulson
MBUS 511, Version 1.2c

Encryption Export: The New Regulations And Their Ramifications.

INTRODUCTION

For decades the United States Government has regulated the sale of encryption technology for national security reasons. The regulations were meant to prevent criminals and other nations from using U.S. encryption technology to thwart the efforts of the National Security Agency and other intelligence/law enforcement agencies. United States encryption companies and developers were greatly restricted, even as recently as last year, in their ability to sell strong encryption technology in the global market. Foreign companies based in nations that do not regulate or loosely regulate the sale of encryption technology have been filling the gap by meeting the ever-increasing demand for encryption tools.

Beginning in 1996, the Clinton Administration made advances toward liberalizing the regulation of encryption technology and began the process of improving the ability of United States firms and developers to compete in the global economy. The administration played close attention to industry concerns and those concerns levied by governmental bodies involved with national security and law enforcement. This approach to drafting the new export regulations along with pressures applied by lawsuits and organizations like the American Civil Liberties Union has resulted in the current status in encryption export regulations.

BACKGROUND

It is important to have an appreciation for just how far the United States has come in a relatively short span of time before leveling any judgments on the viability of the current export restrictions. Prior to 1996 the regulation of encryption exports did not even fall under the Department of Commerce; rather, those duties fell to the State Department. Specifically encryption technology fell under the U.S. Munitions List and was treated as essential to national security, much as blueprints for a missile would be. Much of the Cold War mentality still prevailed.

There were three major cases, which acted as stimuli for the Clinton Administration causing them to review the antiquated manner in which the U.S. government was handling encryption technology export. Professors Bernstein and Junger challenged the constitutionality of the export restrictions citing the belief that it violated their First Amendment right of free speech. By bringing the encryption export regulation debate into an open public forum these men helped to engender support for reform. The "Bernstein vs. Department of Justice ruling in May (1999) is being considered by many the beginning of the end of government encryption controls. Professor Bernstein won the case, stating that his First Amendment rights to free speech were violated when he could not post his strong crypto algorithms on his Web site as an instructional aid in support of his cryptography course"(Reavis, "Encryption Policies are relaxing"). Mr. Phil Karn, a private citizen, also attacked the old regulation those his lawsuit challenged the regulations distinction between the cryptographic source code stored on electronic media and the very same source code when printed on paper in court. "…the book itself is 'in the public domain' and hence outside of their jurisdiction, a floppy disk containing the exact same source code as printed in the book is a 'munition' requiring a license to export. It's old news that the US Government believes only Americans (and maybe a few Canadians) can write C code, but now they have apparently decided that foreigners can't type either!" (Karn). These pioneers highlighted the inequity of the federal governments system of regulations of this specialized technology.

The U.S. encryption companies that had to market their products in accordance to the restrictive guidelines in place in the nineties were also applying pressure on the United States government through congressional representatives. "For years, the U.S. government, lead by FBI director Louis Freeh, has argued that the U.S. must keep a tight lid on the export of data-scrambling products that guard information transmitted via the Internet. …But the high-tech industry is worried that the tough U.S. stance would make it impossible for U.S. companies to compete against encryption products made elsewhere in the world. An industry sponsored study unveiled last June reported that American-made encryption products must compete with 805 products made in 35 different countries" (Perine).

The Clinton Administration began to respond to the pressure for change in 1998 when it relaxed export regulations for financial institutions like banks. An interim rule filed September 21st of 1998 allowed these institutions to distribute within their organizations "non-recoverable non-voice encryption commodities or software of any key length…provided the end-use is limited to secure business financial communications or transactions or financial communications/transactions between the bank or financial institution and its customers" (Majak, Document 98-25096, page 50517) provided that the encryption item in question had been reviewed and licensed for export. On December 3 of 1998 the United States signed the Wassenaar Arrangement which had as its primary function munition export control. "(H)owever, encryption technology is also covered by the (Wassenaar Arangement, and)due in large parts to the efforts of the U.S… set the boundaries for international exports of encryption between the thirty-three signatory nations" (Reavis, "The former Soviet bloc is a mixed bag"). Later that same month, the Department of Commerce published an amendment to the interim rule with a request for comments; the dialogue between the Administration and the U.S. encryption business community began in earnest. There was a great deal of haggling from both sides of the issue: those concerned with the risks to national security/law enforcement and those wanting complete deregulation.

House Resolution 850, also known as the SAFE Act (Security and Freedom through Encryption) was introduced in the summer of 1999 and sponsored by Rep. Bob Goodlatte, R-VA and Rep. Zoe Lofgren, D-CA. The SAFE Act originally called for the complete removal of any controls on encryption export, but it was amended in July 1999 to give the president the ability to ban some forms of encryption technology and to call for strict licensing approval before companies could export the strongest forms of encryption. Officials and agencies within the government fought hard to prevent total deregulation. "…senior Defense Department and intelligence officials warned lawmakers that eradicating the controls on technology would give terrorists and other criminal organizations around the world the means to cloak their plans for carrying out violence in a web of electronic secrecy" (Verton). "The FBI had also sought to tie relaxation of the export rules to concessions allowing the agency access to 'keys' that can descramble encrypted data" (Perine). However one of the reasons the SAFE Act was originally introduced was to

prevent law enforcement from having those very keys and thus ensuring the individual citizen's privacy. The bill garnered quite a bit of support. This support resulted not only in the Clinton Administration deciding that it was time to do a major revision of the export regulations, but also in the FBI backing away from its assertions that encryption was good as long as law enforcement had the keys to read everyone else's data.

The Commerce Department released a draft of the proposed changes to the encryption export regulations for review by industry in November of 1999 and the draft quickly leaked out to the press through industry channels. The proposed regulations were a disappointment to some because of the difficult legalese they were written in. "'The draft regulations make progress, but fall short of the breakthrough announced in September,' said Ed Gillespie, executive director for Americans for Computer Privacy. 'Instead of a clean lifting of export regulations, we have a complicated morass of regulations'" (Perine). The Administration took the comments to heart and made progress toward deregulation when it published the revised version of the export regulations in January of 2000. The important changes included:

1. Encryption Technology of any key length can now be exported without licenses after a one time technical review to any non-government end-user in any country except sanctioned entities, those countries which sponsor terrorism and their nationals. A list of the 7 prohibited countries follows: Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.
2. Encryption Technology of any key length can now be exported to governmental end-users if approved with a license.
3. Internet Service Providers or Telecomm Providers can provide encryption services to the general public without a license. However encryption services specifically for governments will require a license.
4. Encryption source code can be exported without a license provide the Bureau of Export Administration is given a copy or notified in writing of where it can find the Internet location prior to the release of the source code.
5. Encryption Technology of any key length can now be exported to foreign subsidiaries of U.S. firms without technical review. Foreign nationals

working for U.S. firms in the U.S. no longer require an export license.

6. Reporting is now only required when encryption technology greater than 64-bits is exported to a non-U.S. entity and the technology in question is not a retail or finance product for an individual consumer.

(Goodman and Cottilli, "Fact Sheet").

THE NEW REGULATIONS IN A GLOBAL MARKETPLACE

The new export regulations while short of complete deregulation did make life a lot easier for U.S. firms marketing encryption technology globally. "'These rules guarantee the largest access to the world markets for U.S. software security products that we've ever seen'", said Robert Holleyman, president Business Software Alliance ("U.S. relaxes encryption rules"). And the U.S. Government was not the only government making strides forward to liberalize encryption technology export. In a study titled: "Cryptography and Liberty 2000, An International Survey of Encryption Policy." the Electronic Privacy Information Center (EPIC) reported: "'The rise of electronic commerce and the recognition of the need to protect privacy and increase security of the Internet has resulted in the development of policies that favor the spread of strong encryption worldwide. Governments attempting to develop e-commerce are recognizing that encryption is an essential tool for transactions and are reversing decades-old restrictions based on national security concerns…The decision by the United States to liberalize its own encryption export regulations in January 2000 had the effect of weakening the position of those who favor strict controls on cryptography'" (McCarthy).

In October of 2000 the Clinton Administration further relaxed export controls by allowing the 15 European Union (EU)nations and 8 other trading partners to import encryption of any key length without a license and eliminating a 30-day waiting period(Krebs, "New Encryption Regulations Take Effect On Today"). The eight countries included outside of the EU are: Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland, and Switzerland. The EU currently allows its members to export encryption to a set list of 25 nations and makes no distinction between governmental and non-governmental end-users in those nations.

Oddly enough there are nations that are tightening their restrictions on the export, import and even use of encryption. Proposals similar to to the FBI's original demand for encryptions keys are being discussed in countries that include: the United Kingdom, India, Belgium and the Netherlands. Countries, which have broad restrictions of encryption, also tend to place restrictions on the use of the Internet and include: Belarus, Burma, China, Kazakhstan, Pakistan, Russia, Tunisia and Viet Nam. By and large these restrictions are unenforceable and according to "Cryptography and Liberty 2000, An

International Survey of Encryption Policy." a report by EPIC, "The Rapid growth of worldwide electronic commerce and the lack of international consensus on restrictions will further isolate these countries and make it difficult for them to continue these polices…the Internet will make it impossible for them to enforce the laws in any meaningful way without imposing massive surveillance and censorship" (McCarthy).

The evolution of our current regulations stands as a testament to the very real possibility that soon any attempt to restrict the free flow of encryption technology in a global economy will be verging on impossible. The question now is when will governmental institutions within the U.S. and globally reconcile with the emerging face of a borderless marketplace.

WORKS CITED

Goodman, Morrie and Cottilli, Eugene. "Commerce Announces Streamlined Encryption Export Regulations". 12 Jan. 2000. *Linux Today*. 17 Apr. 2000. http://linuxtoday.com/stories/15034.html

Karn, Phil. "The Applied Cryptography Case: Only Americans Can Type!". 6 Mar. 1998. *Phil Karn's Home Page.* 17 Apr. 2001. <http://people.qualcomm.com/karn/export/>

Krebs, Brian. "New Encryption Regulations Take Effect On Today". 19 Oct. 2000. *Newsbytes.* 17 Apr. 2001. <http://www.newsbytes.com/pubNews/00/156920.html>

Majak, R. Roger. "Encryption Items." Federal Register. Vol. 63, No. 183, 22 Sept. 1998. Document 98-25096 of 14 Sept. 1998 (Filed 21 Sept. 1998) U.S. Department of Commerce: The Bureau of Export Administration. 17 Apr. 2001. <http://www.bxa.doc.gov/Encryption/regs.htm>

McCarthy, Jack. "Survey finds encryption rules loosening worldwide". 4 Apr. 2000. *CNN.* (IDG) 17 Apr. 2001. <http://www.cnn.com/2000/TECH/computing/04/05/encryption.idg/>

Perine, Keith. "Cryptic Crypto Rules Uncloaked" 23 Nov 1999. *The Standard.* 17 Apr. 2001. <http://www.thestandard.com/article/0,1902,7836,00.html>

Reavis, Jim. "Trends in government encryption policies". 18 Aug. 1999. *Network World Fusion.* 17 Apr. 2001. <http://www.nwfusion.com/newsletters/sec/0816sec2.html?nf>

Verton, Daniel. "Congress targets exported encryption tech". 23 Jul. 1999. *Network World Fusion.* 17 Apr. 2001. <http://www.nwfusion.com/news/1999/0723crypto.html>

"U.S. relaxes encryption rules". 19 Oct. 2000. *USA Today.* Washington(AP). 17 Apr 2001. <http://www.usatoday.com/life/cyber/tech/cti691.htm>

WORKS CONSULTED

"Civil Liberties Groups Say New Encryption Export Regulations Still Have Serious Constitutional Deficiencies". 13 Jan. 2000. *Electronic Privacy Information Center.* 17 Apr 2001. <http://www.epic.org/crypto/export_controls/draft_regs_11_99.html>

Eckert, Sue E. "Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List." Federal Register. Vol. 61, No. 251, 30 Dec. 1996. Document 96-33030 of 23 Dec. 1996 (Filed 26 Dec. 1996) U.S. Department of Commerce: The Bureau of Export Administration. 17 Apr. 2001. <http://www.bxa.doc.gov/Encryption/regs.htm>

Johnson, John D. "What the lifting of Encryption Technology Restrictions Really Means". 2 Nov. 1999. *Security Portal.* 17 Apr 2001. <http://securityportal.com/direct.cgi?/topnews/encrpt-means.html>

Johnston, Margret. "U.S. frees up encryption policy". 14 Jan. 2000. *CNN.* Washington(IDG). 17 Apr. 2001. <http://europe.cnn.com/2000/TECH/computing/01/14/us.encrption.idg/>

Johnston, Margret. "U.S. Relaxes Encryption Export Policy". 13 Jan. 2000. *PCWorld.* (IDG News Service). 17 Apr. 2001. <http://www.pcworld.com/news/article.asp?aid+14768>

Krebs, Brian. "Encryption Regs may Need "Tweaking"". 4 May 2000. *Newsbytes.* 17 Apr. 2001. <http://www.computeruser.com/news/00/05/04/news7.html>

Majak, R. Roger. "Encryption Items." Federal Register. Vol. 63, No. 251, 31 Dec. 1998. Document 98-34669 of 23 Dec. 1996 (Filed 30 Dec 1998) U.S. Department of Commerce: The Bureau of Export Administration. 17 Apr. 2001. <http://www.bxa.doc.gov/Encryption/regs.htm>

Majak, R. Roger. "Revisions to Encryption Items." Federal Register. Vol. 65, No. 203, 19 Oct. 2000. Document 00-26646 of 11 Oct. 2000 (Filed 18 Oct. 2000) U.S. Department of

Commerce: The Bureau of Export Administration. 17 Apr. 2001. <http://www.bxa.doc.gov/Encryption/regs.htm>

Office of Strategic Trade and Foreign Policy Controls: Information Technology Controls Division. "New Encryption Rules" U.S. Department of Commerce: The Bureau of Export Administration. 17 Apr. 2001. <http://www.bxa.doc.gov/Encryption/regs.htm>

"Ruling: Encryption ban unconstitutional". 5 Apr. 2000. *USA Today.* Cincinnati(AP). 17 Apr 2001. <http://www.usatoday.com/life/cyber/tech/review/crh036.htm>