Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Encryption Regulation: A First Amendment Perspective

Advances in technology have allowed us to move away from traditional paper-based media to the digital communications of the Internet, which has in turn created new challenges to the security and privacy of the data flowing over it. Envelopes and locked filing cabinets are being replaced by cryptographic security techniques such as encryption in an attempt to keep private information private. Through the use of cryptography, communications and information transmitted and stored by computers can be protected from unautho...

Copyright SANS Institute
Author Retains Full Rights

AD

Encryption Regulation: A First Amendment Perspective

Linda K. Mickna

July 23, 2001

Introduction

The methods by which we communicate with each other are changing rapidly. Advances in technology have allowed us to move away from traditional paper-based media to the digital communications of the Internet, which has in turn created new challenges to the security and privacy of the data flowing over it. Envelopes and locked filing cabinets are being replaced by cryptographic security techniques such as encryption in an attempt to keep private information private. Through the use of cryptography, communications and information transmitted and stored by computers can be protected from unauthorized access. Previously, businesses carried out electronic transactions over closed networks, pre-existing contractual relationships were often in existence, and there was little doubt as to the authenticity of the sender or receiver of information. However, with businesses connecting their systems to the outside world via the Internet, the possibilities for interception of communications and theft of information has grown enormously and the need for security and confidentiality has become paramount. As no one government, corporation or person controls the Internet, which spans more than 100 countries and has millions of users connected to it, the Internet cannot be secured, so individual pieces of information flowing over it must be protected, which is best done through the use of encryption. In fact, it has been suggested that the very future of E-Commerce may depend upon the use of appropriate encryption technology.

Background

Cryptography is defined as the science, or art, of secret writing. The term cryptography itself comes from two Greek words, Crypto, meaning *hidden*, and Graphia, *writing*. The practice of encryption has a long history going back thousands of years predating Caesar's reign in Rome when the method used was based upon replacing the letters of the alphabet with another letter, for example, ROT-13, whereby a different letter 13 characters ahead substitutes for each letter. Although simple, this method was effective until the code was cracked. Cryptography has been particularly important during wartime, when it has been used to protect espionage communications. Encryption devices such as the German Enigma machine were used to encode and decode messages during World War II until cryptographers broke the code.

Early encryption was relatively secure because computers lacked sufficient power to quickly calculate all possible solutions. However, 40-bit algorithms that used to take months to decode can now be broken in a fraction of the time. For example, two French graduate students were able to break Netscape's 40-bit algorithm using idle time on a computer at the Ecole Polytechnique in Paris in a matter of days without incurring any cost to themselves or the school. A Corporation, foreign government, terrorist organization, drug operation, or any other entity with the necessary financial resources could break a 56-bit DES key in about 12 seconds (Samoriski et al., "Encryption and the First Amendment").

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The methodologies in use today are far more complex, involving the use of mathematical algorithms. The messages being encrypted are no longer limited to paper-based communications, but may be a stream of bits, a text file, a bitmap, a stream of digitized voice or a digital video image. The technology is embedded in the magnetic strips of credit cards, in the browsers used to navigate the Internet and in the e-mails we send to each other. And in addition to ensuring confidentiality, encryption also provides for authentication and non-repudiation, which are important to the acceptance of e-signatures.

Encryption today, therefore, is integral to the way the world does business. The Internet and E-commerce have created a new realm for encryption, one where it is not an object used almost exclusively by government agencies, but rather an important tool in providing privacy and security for business and personal transactions. It provides the "packaging" that allows for secure business transactions over the electronic superhighway.

Policy Issues

The policy issues surrounding encryption controls essentially involve the balance between the government's need for intelligence and law enforcement capabilities and the privacy and speech interests of individuals and entities involved in electronic communications and commerce. This balance is a delicate one that is not easily maintained.

Until recently, the federal government has tightly regulated the export of encryption technology. The primary concern with the unregulated export of strong commercial encryption technology is that the encryption of communications and financial transactions will hinder law enforcement and frustrate national security objectives. In the government's view, if encryption is not regulated, it will be used by terrorists, organized crime, drug dealers, child pornographers and other potentially dangerous groups to commit crimes and avoid detection. Encryption poses unique problems for investigators and regulators in their attempts to monitor unlawful practices as it prevents monitoring by government officials.

There is a growing citizen movement that has sought to place limits on governmental regulation of encryption because of privacy, free speech and copyright issues. Internet users and on-line public advocacy groups have joined together in an attempt to influence policy makers in Washington to advocate an Internet free of government regulation.

Powerful and often interconnected corporate groups also attempt to influence encryption policy. The industry, which includes software developers, computer equipment manufacturers and the communications and financial services companies, has an economic interest in the debate. Encryption is particularly important in keeping financial transactions secure, which is a consideration for those making purchases on the Internet. Export restrictions may translate into a multi-billion dollar loss to computer and software companies.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

What is particularly interesting about the context of this debate is the unlikely combination between citizen groups and private industry, which have united in their quest to keep encryption unregulated. During the 1960's and 1970's environmental, health and safety issues divided corporate and public interests, creating an adversarial relationship, but in this case industry interests have aligned themselves with Internet users and public interest groups because it is a means to an economic end.

First Amendment Analysis

The First Amendment to the U.S. Constitution provides as follows:

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

There are three fundamental questions that must be raised when considering the encryption debate from a First Amendment perspective: Is encryption speech? If so, what is the government's interest in regulating it? And what is the proper standard to apply when determining how the government may regulate encryption?

I. Prior Cases

The Courts answered the first question in *Daniel J. Bernstein v. United States Department of State*. Daniel Bernstein was a graduate student who developed an encryption program called "Snuffle" and wrote a descriptive paper, instructions for programming Snuffle, and a computer program that used Snuffle. All three were considered controlled encryption items under then-current regulations. Bernstein alleged the government violated his right to free speech by restricting his ability to post an encryption program on the Internet. In her ruling, District Court Judge Marilyn Patel held that computer language, like all other forms of language, is entitled to First Amendment protection. Source code, in the judge's opinion, is speech. In her words, "This court can find no meaningful difference between computer languages...and German or French. All participate in a complex system of understood meanings within specific communities."

In *Junger v. Daley* the Sixth Circuit Court stated that because "computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment."

Other cases have classified similar items as speech. In *Ward v. Rock Against Racism*, the Court said "music, as a form of expression and communication, is protected under the First Amendment." In *Texas v. Johnson*, the Supreme Court classified flag burning as speech after deciding it was "sufficiently imbued with elements of communication to fall within the scope of the First and Fourteenth Amendments." In *United States v. The Progressive*, technical information in the Progressive magazine article about hydrogen

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

weapons were considered speech. In *Ynigue z v. Arizonans for Official English*, the court held that "Language is by definition speech, and the regulation of any language is the regulation of speech" and "the choice to use a given language may often simply be based on a pragmatic desire to convey information to someone so that they may understand it." It is not such a great leap from considering music, technical information and languages to be speech subject First Amendment protection to the conclusion that encrypted messages containing elements of communication fall under the same category (Samoriski, et al, "Encryption and the First Amendment*)*.

II. The Government's Interest

As previously stated, the government's concern with widely available encryption is that the encoding of communications and financial transactions will negatively affect law enforcement and national security. There is evidence that drug traffickers, organized crime and international terrorists currently use encryption to protect communications and hide financial transfers. In 1999, the FBI estimated that five percent of its investigated cases involved the use of some encryption technology wherein the criminals attempted to mask communications. This number does not include investigations by the other U.S. security agencies (i.e. the NSA, CIA) that are impeded by the use of encryption. The number of criminal cases employing encryption technology is expected to grow dramatically as encryption technology becomes more readily available in the marketplace (Butler, "Safe and Legal E-Commerce: Legal and Regulatory Issues Raised by the Use and Export of Encryption Technology).

Some government agencies have suggested a system of "key escrow" or "key recovery" whereby decryption keys or parts of keys would be deposited with either a governmental agency or a private entity (a trusted third party). Upon the showing of a need to decrypt a particular communication, such as pursuant to a search warrant or other court order, the government would be given access to the key from the agency or third party in order to decipher the message.

It seems reasonable that the government should be allowed to use wiretaps upon a reasonable showing of probable cause and law enforcement agencies must be able to intercept communications of those who engage in criminal activity or acts of terrorism. The NSA and the FBI are charged by Congress with the responsibility for defensive intelligence missions, and should therefore have the ability to intercept and decode encrypted messages when those messages contain information that threatens national security. Regulation of encryption may be a means to that end.

However, the government's interest in regulating encryption is not absolute in a democratic society. The interest varies depending upon whether we are at war or at peace, whether the communications are commercial in nature or between private citizens, whether the speech is part of the functions of a free press, etc. The government does not have a compelling interest in intercepting and decoding all messages in all circumstances.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The government's reliance upon a law enforcement/national security rationale for regulating encryption falls short for other reasons as well. For one thing, law enforcement methods of investigation do not rely solely on cryptography. Also, mandated key escrow would have depressed the development of encryption technology in the U.S., providing other countries that do not regulate encryption with competitive advantages.

III. What is a Reasonable Standard?

There have been other instances when the Court has addressed the First Amendment versus the government's interest in national security, so we can look to existing standards for the appropriate one to apply to the encryption issue. The "clear and present danger" test provides a basis for a consideration of the government's ability to limit speech. In the *Schenck* case, where the defendants were accused of attempting to obstruct the draft during World War I, Justice Oliver Wendell Holmes spoke about when speech is not protected by the First Amendment, "The question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent. When a nation is at war many things that might be said in time of peace are such a hindrance to its effort that their utterance will not be endured so long as men fight and that no court could regard them as protected by any constitutional right." In the later *Abrams v. United States* case Justice Holmes indicated that opinions should not be suppressed "unless they so imminently threaten immediate interference with the lawful and pressing purposes of the law that an immediate check is required to save the country." The idea that the danger must be imminent was for a time forgotten by the court during the anti-Communist fervor, but it was reinstated as the fervor died down.

Under current standards the government must show objective proof of a serious danger and provide convincing evidence that the danger is immediate and not remote before it may halt speech. When this standard is applied to the government's argument that unless it is allowed to regulate cryptography, terrorists, organized crime leaders and drug dealers will use encryption as a tool, it is obvious that these dangers are speculative and remote. In fact, similar arguments have been made in the past about books and magazines, which also failed to sway the court because of the First Amendment.

The government, then, has a heavy burden of proof to overcome before it can impose encryption standards upon society. Even in the midst of war it must meet certain standards before it could "search and seize" in Cyberspace (Samoriski et al., "Encryption and the First Amendment").

Conclusion

The implications of the technology and the problems the technology presents are enormous and complex. In the past, the use of cryptography was limited primarily to government entities involved in the top-secret business of sending, receiving, and

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

attempting to intercept and decrypt the messages of others. The growth of the Internet has created other interested parties, such as banks, corporations, organizations and individuals with access to sophisticated technology. Huge amounts of highly sensitive information are passing across the Internet, which is an unsecured public network. With the proliferation of encryption the government's monopoly on its use has ended and the security of its own communications and national security are in question. At the same time, public concern about privacy in all areas has been growing in recent years. It is not surprising that these different interests would clash.

It is unlikely that the courts will treat encryption as a separate form of speech. The government is required to present a very compelling case to the Supreme Court to justify encryption regulation that infringes upon the First Amendment. Justice Brandeis, in his opinion in *Whitney v. California* spoke about the clear and present danger doctrine, "Fear of serious injury cannot alone justify suppression of free speech and assembly. Men feared witches and burnt women. It is the function of speech to free men from the bondage of irrational fears." Without a "clear and present danger" government agencies should not be allowed unlimited access to private conversations. The danger to society is far too great.

List of References

Butler, James W. III, "Safe and Legal E-Commerce: Legal and Regulatory Issues Raised by the Use and Export of Encryption Technology", Legal Issues in Information System Security: Privacy Protection & Piracy Prevention, Pennsylvania Bar Institute, 2000.

"Cryptography and Liberty 2000: An International Survey of Encryption Policy", April 3, 2000. Electronic Privacy Information Center.
http://www2.epic.org/reports/crypto2000/

Paulson, Victorian F. "Encryption Export: The New Regulations and Their Ramifications", May 1, 2001.
http://www.sans.org/infosecFAQ/encryption/export.htm

"Perspectives on Security In The Information Age", Computer Systems Policy Project, January 1996.
http://www.cspp.org/reports/report1-96.html

Samorski, Jan H., Huffman, John L., Trauth, Denise M. "Encryption and the First Amendment".
http://www.umd.umich.edu/casl/hum/comm/crypto~1.htm

Taylor, David, and Ortiz, Felix A. "Encryption – hindering the hackers; some technical and legal issues", Legal Issues in Information System Security: Privacy Protection & Piracy Prevention, Pennsylvania Bar Institute, 2000.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**