

## Cyberlaw Term Paper

Marian Gorman

# Overview of Data Encryption and Legal Issues

What is encryption and why do we need it?

The concept of encrypting information has been popular for hundreds of years. Revolutionaries, scientists, political activists and lovers have utilized this technique to maintain privacy and confidentiality in their communications. As kids, we would take our secret messages and shift the letters of the alphabet by a specific number to create an encrypted message. For example, by shifting the letters of the alphabet by three we could change the word cyberlaw to fbehuodz. In encryption, a message is referred to as plaintext before changing it in any way. Data encryption is the process whereby plaintext data is converted to ciphertext data. Ciphertext data can only be read by a party with a secret decryption key. A method for encrypting text is referred to as a cryptosystem. There are many uses for encryption today, particularly, with the widespread use of the Internet. Encryption is used to verify messages, validate and authenticate users and authorize transactions.

Banks use encryption to secure customer identification numbers at ATM machines.

All U.S. electronic funds transfer messages are encrypted. Online vendors depend upon the security of credit card transactions in conducting business. Many political groups use cryptography to protect the identity of online users. Internet users want electronic privacy; freedom from observance by the government or other parties. Anonymity is vital to both privacy and freedom of speech.

Potential Abuses of Encryption:

The U.S. Government is concerned with the abuse of this technology at the hands of criminals, terrorists and hostile foreign governments. Encryption could impede their efforts to gather information and monitor the communications related to illegal enterprises.

It is believed that unbreakable cryptography could seriously hinder the efforts of law enforcement and threaten public safety.

### Export Controls:

In 1988, The U.S. initiated export controls of encryption source code. The Arms Export Control Act regulates the exports of defense articles and services to promote world peace and security. Congress authorized the President to designate a list of defense articles to be restricted from export. The U.S. State Department included cryptographic systems, equipment, assemblies, modules integrated circuits, components or software capable of maintaining secrecy or confidentiality of information or information systems as defense articles. This has restricted distribution of dangerous technologies to assure that encryption programs are not available to criminals and governments overseas.

### Keys:

The key to a cryptosystem is a specific value that converts the plaintext to ciphertext and allows the ciphertext to be transformed back into plaintext. Popular techniques depend upon both the sender and receiver having knowledge of the secret key. This technique is known as secret key or symmetric encryption. A security consideration with this method involves the communication or transfer of the key between sender and recipient.

### Public Key System:

A public key system utilizes two keys, one public and one private. Sender and recipient have both keys. The private key must be kept secret and the public key is publicly known.

These keys are related through a mathematical algorithm. The sender encrypts his message with his private key and the recipient decrypts it with the sender's public key.

Anyone who has been given the sender's public key can in return send him an encrypted message. The advantage to this type of encryption lies in the fact that each user has only one key to encrypt and decrypt messages that they send or receive.

### DES (Data Encryption Standard):

Stream and block cyphers are two types of symmetric encryption algorithms (formulas).

The length of a key is determined by the number of bits of data. If a key is long and contains more bits, then it is considered more difficult to break. Stream ciphers encrypt one bit of text at a time. Block ciphers can encrypt numerous bits of data at one time.

A block consists of 64 bits. DES (Data Encryption Standard) is a secret key system that is endorsed by the US government. It was designed in the 1970's and is still popular today.

It is a block cipher containing a 64 bit block and has a 56 bit key. This would provide approximately 72 quadrillion different possible keys. (<http://www.whatis.com/des.htm>)

Export of the DES is strictly regulated by the U.S. State Department. There has been recent criticism that DES is becoming less secure. In 1997, RSA Data Security had issued a challenge, offering \$10,000 to decode a message encrypted using DES. A group consisting of tens of thousands of computer across the U.S. and Canada linked together using the Internet and managed to decrypt this message. It used a technique referred to as "brute force". Participating computers tried every possible decryption key. The code was cracked in approximately 20 days. Principle organizer, Rocke Verser, is a self-employed contract programmer from Colorado. Verser wholeheartedly agrees with the sentiment expressed in RSA Data Security's secret message, "Strong cryptography makes the work a safer place. (<http://www.frii.com/~rcv/despr4.htm>)

The Clipper Chip:

The Clipper Chip is an encryption method proposed under the Clinton Administration. It is known as an Escrowed Encryption Standard that utilizes a symmetrical algorithm that is classified. It is based on a tamper resistant hardware chip that uses an NSA designed algorithm. This is used in combination with a technique that enables any communication that has been encrypted with the chip to be decrypted through a special chip with a unique key and a special Law Enforcement Access Field. This field would be transmitted with the encrypted communication. The government originally intended to install the chip in all fax, telephone and modem technology; to have it become a national standard. U.S. law enforcement agencies could decrypt any messages that had been encrypted by utilizing the Clipper Chip. This would only be done with due authorization. Naturally, this chip was opposed by many civil liberty groups as an infringement upon the privacy of users.

A new version of the Clipper Chip proposal appeared in 1995. Clipper II would keep the present export ban on strong encryption tools yet would permit the export of moderately strong systems containing key escrow systems.

In 1996, the U.S. government published a new proposal intended to create a public key infrastructure for encryption. This new proposal (Clipper III) would enable users of encryption to identify the people with whom they are communicating. Many view this as an important step for the widespread use of secure electronic communications. Users of this system would have to guarantee access to the encryption keys with an approved key escrow agent. Privacy and security from the government observation are crucial issues. Should this chip become the standard, the government would be capable of examining email and the determining the recipients of these messages.

Issues of Free Speech:

John A Fraser, in his paper entitled "The Use of Encrypted, Coded and Secret Communications is an Ancient Liberty Protected by the United States Constitution" (<http://vjolt.student.virginia.edu/graphics/vol2art2.html>) presents an interesting discussion of the use of encryption by the founding fathers of this country and traditional uses of anonymity. In colonial America, secret communications were used to elude the efforts of government agents and censors. In 1748, Benjamin Franklin printed a text on the use of codes, ciphers and secret writing. At that time, there was a government practice of opening and reading private mail. Also, letters could be stolen from the post riders. Thomas Jefferson frequently used encrypted communications to protect his private thoughts and to convey confidential information.

In the 1800's a strong demand for cryptographic developments continued and it was met with host of different methods and competing suppliers. Fraser points out that,

"until 1960, there is no evidence that the federal government believed it should exercise its powers to restrict the use of encryption technology by private citizens."

The NSA has claims that its initiatives to restrict access to sophisticated and advanced encryption techniques have been based upon policies of denying knowledge for the protection of the public, for economic efficiencies and for uniformity in computer information security. Over the last ten years, Americans have been able to protect and secure their communications with easier to use encryption

methods. These methods have been able to frustrate the interception attempts of many sophisticated government agencies.

In response, the government has pushed through Congress a law requiring telecommunications carriers to modify networks so that federal agencies can install wiretaps. The Clinton Administration has introduced the controversial Clipper Chip.

Finally, the government has a very aggressive program to enforce the munitions export regulations against advanced encryption software products. ITAR (International traffic in Arms Regulations) routinely denies export permission of encryption products stronger than the DES standard that has been approved by the government. These restrictions deny American business the chance to compete in the international market for advanced encryption technology. It is assumed that the government wants to restrict domestic development of technology to limit what the government wants its citizens to own and use.

Constitutional or Unconstitutional?

Americans have enjoyed the right to speak freely and with privacy since adoption of our Constitution. Arguments against restricting the use of encryption technology allege violations of our Constitutional Rights. The First and Fourth Amendments protect our rights to free speech and to feel secure in our persons, houses papers and effects against unreasonable searches and seizures. The Fifth Amendment protects our rights to life, liberty and property with due process.

Encryption source codes (the programming text for software) represent a form of speech.

As such, they should be protected from export controls and government mandated requirements. ([http://vjolt.student.virginia.edu/graphics/vol2/vol2\\_art2.html](http://vjolt.student.virginia.edu/graphics/vol2/vol2_art2.html))

Free speech advocates have vocally criticized the restrictive encryption policies of the government.

Bernstein v. U.S. Department of State:

In the case of Bernstein v. U.S. Department of State 945 F. Supp. 1279(N.D. Cal 1996),

Bernstein brought action against the Department of state seeking injunctive relief from the

enforcement of the Arms Export Control Act and the International Traffic in Arms Regulations (ITAR) on the grounds that they are unconstitutional. Bernstein, a Phd candidate at the University of California at Berkeley working in the area of cryptography.

He had developed an encryption algorithm called Snuffle, a private key encryption system.

He had written a paper entitled "The Snuffle Encryption System" and had also written the source code in a programming language "C". Cryptographic equipment is classified and listed on the U.S. Munitions List that require a license for exporting. The paper and written instructions were not included on the munitions list. The court, in this case, found computer source code to be a form of speech. The Department of State argued that source code was "unprotected conduct". According the court:

"Speech in any language consists of the expressive conduct of vibrating one's vocal chords, moving one's mouth and thereby making sounds or of putting pen to paper, or hand to keyboard. Yet the fact that such conduct is shaped by language - that is, a sophisticated and complex system of understood meanings - is what makes it speech. Language is by definition speech, and the regulation of any language is the regulation of speech. Nor does the particular language one chooses change the nature of language for First Amendment purposes. This court can find no meaningful difference between computer language, particularly high level languages as defined above, and German or French." ([http://samsara.law.cwru.edu/comp\\_law/bern970825dec.html](http://samsara.law.cwru.edu/comp_law/bern970825dec.html))

The U.S. District Court for the Northern District of California granted injunctive relief from NSA export controls and found that these controls impermissibly limit free speech.

Conclusion:

Free speech advocates argue that the transmission of encryption source codes represent a form of scientific speech. The information that software developers want to transmit represents the results of their research in cryptography. It is the transmission or communication of the encryption techniques that the government wishes to restrict, not the communication.

Restrictions resulting from concern for national security may be eroding First Amendment protections. Scientists will be denied the freedom to express and discuss developing technologies. Future legal cases will continue to raise objections based on free speech issues. In turn, the courts will be challenged to develop and redefine free speech doctrines in determining whether our current policies are overbroad in dealing with national security issues. Software developers argue that alternate forms of control could better serve security interests. Technology currently exists to control access to Internet distribution sites.

The market forces of global economy have increased pressures on information technology.

Increasing demand for development of encryption software will only accelerate. These technologies are already available outside the United States. Market forces will also increase the demand for this software to be freely distributed over the Internet.

The availability of encryption codes will encourage a larger population of users to encrypt communications and will provide businesses worldwide a way to conduct transactions securely.

Arguments are made that the control of source code export discriminates against software distribution as opposed to encryption in print form. This greatly limits the expression of scientific ideas and thereby limits the marketplace for ideas.

The ability to remain anonymous is important to free speech and our right to privacy in communications on the Internet. If Clipper chips and escrow accounts become the standard, the U.S. government will be able to read private e-mail and determine the recipients. This would be a frightening departure from our proud tradition of preserving privacy in our communications and encouraging the free exchange of ideas and information.