Computer Security and the Law:
Regulating the Export of Encryption

TiTi Nguyen

Of all aspects of computer security, none have been more regulated by the government than encryption. Although these regulations have been in place since the end of World War II, the United States' policy towards the export of encryption has increasingly been reexamined because of the growth of computer and Internet usage. At issue is balancing national security and economic interests in order to determine the extent to which the government can, and should, regulate encryption. The trend over the years has been to loosen regulations, despite resistance from the government. What remains to be seen is if this trend can continue in the face of such adamant government resistance and in light of the Sept. 11 events.

Past and Present Encryption Policies

The government began to regulate encryption after World War II. While domestic use of encryption remained (and pretty much still remains) unregulated, the export of encryption technology was forbidden and encryption was classified as a munitions (Baladi 1999). Eventually, new regulations were implemented that allowed for some flow of encryption products. One such regulation was the International Traffic in Arms Regulations (ITAR)(1996). Implemented by the State Department, ITAR was the regulating arm of the Arms Export Control Act (1994), which gave the President the authority to control "the import and export of defense articles…and to provide foreign policy guidance to persons…involved in the export and import of such articles" (Baladi 1999). Any item the President designated as a defense article was put on the United States Munitions List (USML), a list of items that required import and/or export licenses. Encryption technology was one such commodity placed on the USML. Any product that operated with 40-bit encryption or less could be exported freely, but to manufacture or export stronger encryption required a government-issued license (Baladi 1999; Radlo 1996; Klopfenstein 1999: 780-781). Bit encryption involves the number of 0s and 1s used to encrypt data that has been stored electronically. The more bits used to encrypt, the

Law and Society Review at UCSB, Volume 1 (2002).

harder the "key," or the exact bits used to scramble the message, is to figure out in order to descramble the message.

The State Department initially oversaw the encryption export regulations. In 1996, Executive Order 13,026 ("Administration of Export Controls on Encryption Products") transferred jurisdiction of nonmilitary encryption products to the Commerce Department (Soma and Henderson 1999: 106). While encryption items on the USML were still regulated by the State Department, the rest of the encryption the remaining regulations, citing the harm of these regulations to economic interests and Constitutional liberties. There are many reasons for support of or opposition to continued government regulation of encryption.

Support for Encryption Regulations

The government's primary concern is the use of encryption to threaten national security, while law enforcement's concern is its ability to conduct electronic surveillance against such criminals and terrorists. Pasko (2000) writes:

> While encryption offers American industry a tremendous advantage in conducting its business by ensuring that transactions and industrial secrets are kept safe, encryption also offers many opportunities for misuse. Criminal activities that use encryption technology to their advantage, such as terrorism, organized crime, and industrial espionage have prompted the federal government to enact strong laws regulating encryption in order to prevent such misuse. (337)

In addition to potential misuse, the government and law enforcement are worried about law enforcement's ability to collect evidence that has been encrypted. They argue that law enforcement agencies do not have the resources or time to conduct brute force attacks to recover keys used by drug traffickers, child pornographers, and information terrorists. Baladi (1999) writes that "[t]he Department of Commerce and the FBI are concerned that the proliferation of encryption will make it more difficult to monitor and apprehend terrorists, which will threaten the security of the United States." Moreover, Smith (1999/2000) notes that "[a]bsent some form of key recovery or recoverable method, a brute force attack will not meet law enforcement needs" (16). Thus, they support the limits on encryption strengths, built-in key recovery systems, and key escrows, where encryption keys can be deposited and held for future reference.

The government and law enforcement assure that proper procedures have been implemented in order to protect Constitutional Rights. The supporters acknowledge the Constitutional and economic concerns related with regulating encryption, but the balance of rights must weigh in favor of maintaining public safety.

Support Against Encryption Regulations

Industry has historically disliked government regulation of free market competition. However, the limits on key lengths that can be manufactured and/or exported, government review prior to manufacturing, and the necessity of a government-issued license prior to exporting, have put high-tech industry at a disadvantage to foreign firms who have no such restrictions. Black (2001) writes, "[s]ome critics contend that, because of U.S. restrictions, the industry has already lost more than $65 million" (297). These regulations affect the industry's ability to protect business transactions from corporate espionage or fraud, as well as to attract new clients. The industry argues that since stronger encryption is being created outside of the United States, it cannot compete at an international level, nor can it take advantage of the same kinds of security its international competitors are using.

Privacy is also a key issue for protesters of encryption regulation. The main reason for encryption is to maintain private and confidential information. This purpose would be defeated if anyone else, even law enforcement, could easily decipher the key. Additionally, the protestors do not believe the government can, or should be, trusted to not abuse its access to key recovery methods, no matter what procedural protections have been implemented. Whether the recovery methods are through "back doors" into the encryption algorithm or through key escrow, which is depositing encryption keys to a government or independent agency, the protesters believe government would be too tempted to use these recovery methods without proper supervision or accountability. Baladi (1999) argues, "there [would be] no difference between mandating key escrow for encryption software and mandating key escrow to our homes." Since escrowing house keys has never been acceptable, even against the government's argument of national security and public safety, encryption keys should not be considered any different (Baladi 1999).

Civil libertarians are also concerned with Constitutional violations that may incur as a result of encryption regulations. Foremost is the right to privacy that has been interpreted from the Fourth Amendment. Another concern is the possible abuse of Fourth

Amendment search and seizure restrictions. The civil libertarians are not convinced the government would use "back doors" into encryption algorithms only if it was given proper authority by the courts. Instead, they believe the government would abuse its access and decrypt encrypted messages before bothering to gain court approval. The First Amendment right to free speech could be implicated in the government's ability to restrict or deny a request to manufacture or export encryption code. This issue has slowly entered the court system, and different courts have come to different conclusions about whether encryption source or object code constitutes speech. The government cannot regulate encryption if it constitutes speech, but can if it does not. Finally, the Fifth Amendment's right to not self-incriminate has also become a contentious issue. The argument is that by requiring the escrow of the encryption key, the government would be compelling depositors to turn over potential evidence against themselves because the key would allow law enforcement access to possibly damaging evidence.

Analyzing the Need for Encryption Regulations

While the government does have a valid need to protect national security and to help law enforcement fight crime, limiting the kinds of encryption that can be manufactured, imported or exported, will not do this. Instead, these limits not only hurt economic and technological interests, but also the very people the government is intent on protecting from harm.

Economic and technological interests are hurt because domestic businesses cannot compete with international firms that offer better and stronger encryption with less government intrusion. These businesses include those that manufacture and sell encryption products, as well as those that use encryption as part of their services. In addition, not only do these businesses lose users because they cannot guarantee better encryption of data, they also lose the ability to protect their own transactions from possible violations of privacy and confidentiality. This also true for individuals, who also cannot take advantage of the protection stronger encryptions afford them.

The violation of privacy because the government allows only weak encryptions is made worse by the government's insistence on key-recovery methods and escrow systems. Not many are willing to trust that the government would diligently protect Constitutional Rights and not abuse these privileges. Also, it is not likely that illegitimate users will "play by the rules," use weak encryption or allow for key-recovery methods to help law enforcement catch them

in the act. Moreover, it is unlikely that international terrorists will use the weak encryptions that are allowed by the U.S., when much stronger encryptions are available outside of the U.S.

Furthermore, regulating the flow of information is a losing battle. The Internet has the ability to distribute anything from anywhere, thus many stronger encryption products than what the U.S. government is allowing are already widely available! (Sehgal 1999: 82). In addition, the ability to distribute encryption products to a large audience would also allow a large audience to review the encryption code. Open source critique is good because it helps improve the product by finding flaws and gives a better understanding about how the code works, both kinds of knowledge the government could use to its advantage to protect national security.

Finally, it is laughable that the government claims it cannot recover keys from strong encryptions in a timely or resourceful manner. As history shows, such as when the Allied forces wanted to crack the German's Enigma encryption machine, when the government devotes its focus on one thing, it will be sure to get it. Additionally, claims that strong encryption, such as 128-bit keys, may take "a trillion years to break with current technology" are equally as absurd (Baladi 1999: Footnote 35). At one point, 40-bit keys were thought impossible and impractical to break, yet it now can be done in under 4 hours, and 56-bit keys were thought secure, yet these too can now be broken with the resources the government has—and within reasonable time frames. Soma and Henderson (1999) emphasize this position:

> The encryption debate also poses the question of whether strong encryption applications…can be broken…. A University of California at Berkeley student broke [a 40-bit PGP-encrypted message] using 250 workstations tied together for a brute force attack. The 250 computers broke the code in 3.6 hours. The National Security Agency ("NSA") used this information to explain that, in comparison to the 40-bit key, the 56-bit technology was virtually unbreakable.
>
> …
>
> Philip Zimmermann testified that Northern Telecom of Canada engineers developed a special chip to crack 56-bit DES codes. These chips, if linked with 50,000 similar chips at a cost of $1 million, could try every 56-bit DES key in seven hours. For a $10 million investment that time

> could be reduced to twenty-one minutes, and for $100 million, just two minutes. Furthermore, Zimmermann made the point that NSA resources could probably reduce that time to a few seconds." (126-127 [footnotes omitted])

Thus, technology will soon, or already is, available to break strong encryptions.

The government is rightfully concerned that strong encryption could be used to harm national security as well as to evade the law. This concern has been heightened in the past months since Sept. 11, as the government has detained hundreds for questioning, planned for military tribunals with secret evidence and no appeals process, expanded wiretapping capabilities, and allowed the taping of privileged lawyer-client conversations (Rosin 2001: A1; Pincus 2001: A6; Lancaster 2001: A1; "An Affront to Democracy" 2001: A24; Lardner and Slevin 2001:A1). All of this has happened in the name of national security. It is not inconceivable for the government to revoke these looser regulations in favor of tighter restrictions on what kinds of encryption can be exported. What the government must not also forget is that in preventing possible terrorists from using these products for harm, it is also preventing possible victims from using these products for protection.

Conclusion

The debate over regulating encryption will undoubtedly continue as the regulations become tighter or looser. What must also continue is the constant questioning about these regulations and the need for the government to justify its intrusion. While the government does have an interest in protecting national security and aiding law enforcement's fight against criminals, this should not come at the cost of stunting economic and technological growth, as well as the careless violation of Constitutional Rights.

References

"An Affront to Democracy." *Washington Post, A24*.

Baladi, Joe (1999) "Building Castles Made of Glass—Security on the Internet," 21 *University of Arkansas at Little Rock Law Review* 251.

Black, Tricia E. (2001) "Note: Taking Account of the World As it Will Be: The Shifting Course of U.S. Encryption Policy," 52 *Federal Communications Law Journal* 289-313.

"Commercial Encryption Export Controls." Information Technology Division,

Office of Strategic Trade and Foreign Policy Controls, Department of Commerce. Available: http://www.bxa.doc.gov/Encryption/Default.htm. [2001, Dec. 7].

Crain, Norman Andrew (1999) "Bernstein, Karn, and Junger: Constitutional Challenges to Cryptographic Regulations," 50 *Alabama Law Review* 869-909.

Klopfenstein, Dena R. (1999) "Deciphering the Encryption Debate: A Constitu tional Analysis of Current Regulations and a Prediction for the Future," 49 *Emory Law Journal* 765-807.

Kluber, Berne C. (2001) "Global Distributions: The Effect of Export Controls," 21 *Houston Journal of International Law* 429-66.

Lancaster, John (2001, October 25) "House Approves Terrorism Measure." *Washington Post,* A1.

Lardner, Jr., George and Peter Slavin (2001, November 14) "Military May Try Terrorism Cases." *Washington Post,* A1.

Moerke, Katherine A. (2000) "Free Speech to a Machine? Encryption Software Source Code is Not Constitutionally Protected 'Speech' Under the First Amendment," 84 *Minnesota Law Journal* 1007-49.

Pasko, Mark T. (2000) "Note: Re-Defining National Security in the Technology Age: The Encryption Export Debate," 226 *Journal of Legislation* 337.

Pincus, Walter (2001, October 21) "Silence of 4 Terror Probe Suspects Poses Dilemma for FBI." *Washington Post,* A6.

Radlo, Edward J. (1996, February) "Legal Issues in Cryptography." Palo Alto, CA: Fenwick & West.

Rosin, Hannah (2001, September 28) "Some Cry Foul as Authorities Cast a Wide Net." *Washington Post, A1*.

Sehgal, Cassidy (1999) "The Power of the Federal Government in the Electronic Age," 4 *Texas Review of Law & Politics* 77-82.

Smith, Charles Barry (1999/2000) "Current U.S. Encryption Regulations: A Federal Law Enforcement Perspective," 3 *New York University School of Law Journal of Legislation and Public Policy* 11-20.

Soma, John T. and Charles P. Henderson (1999) "Encryption, Key Recovery, and Commercial Trade Secret Assets: A Proposed Legislative Model," 25 *Rutgers Computer and Technology Law Journal* 97-134.

Wolfe, D. Forest (2000) "Comment: The Government's Right to Read: Maintaining State Access To Digital Data in the Age of Impenetrable Encryption," 49 *Emory Law Journal* 711-44.

Statutes Cited

Arms Export Control Act, 22 U.S.C. 2751-99 (1994).

Export Administration Act, 50 U.S.C. 2406 (1994).

Export Administration Regulations, 15 C.F.F. 730-774 (1996).

International Traffic in Arms Regulations, 22 C.F.R. 120.1-130 (1996).

President, Proclamation, "Administration of Export Controls on Encryption Products, Executive Order 13,026," (1996).