The Development of Encryption Law in the United States

Introduction

The importance of the Internet in American society and its economy triggered an increase in the amount of Internet-related legislation by the 104th Congress and its successors. At that time, one in three Americans had access to the Internet. Access and activity in cyberspace increased as time progressed. The U.S. Department of Commerce stated that online sales escalated from $3 billion in 1997 to $9 billion in 1998.[1] North American Retailers reflected approximately $4.4 billion in the first half of 1998 alone. As the number of on-line sales increased, the number of Web users worldwide continued to grow as well. From 1998 to 1999, worldwide Web users increased by 55 percent, the number of Internet hosts rose by 46 percent, the number of Web servers increased by 128 percent, and the number of new Web address registrations rose by 137 percent.[2]

It is clear that not only had the numbers increased in the past, but that they would likely continue to grow throughout the new millennium. In fact, the International Data Corporation estimated that revenues of U.S. Internet service providers would continue to rise at a compound annual rate of 28 percent through 2003.[3] Due to the lack of legal precedent in the new era of digital communication, the on-line industry was essentially self-regulated, and remains that way to a great extent.[4] As a result, the law and the need for stricter regulation in cyberspace materialized.

With the increase in Internet activity came an increase in highly

---

1. *Industry Self-Regulation: The 1999 FTC Report to* Congress, 79 CONG. DIG. 41 (February 2000).

2. *Electronic Commerce: Worldwide Growth of the Digital Economy,* 79 CONG. DIG. 37 (February 2000).

3. *See id.*

4. *Foreword: Internet Privacy: Protecting Personal Information Online,* 79 CONG. DIG. 33 (February 2000).

controversial issues. Congress was faced with issues including gambling, pornography, and national security. Congressional bills were introduced in an attempt to regulate commerce by establishing standards for business conduct. Despite unsettled resolutions to such controversies, many still sought to nurture competition as companies moved to deliver high-speed Internet access. Through cable television networks and upgraded telephone lines, the competitors sought new ways to obtain leverage. A "tug-of-war" had begun as to the limits and boundaries to be placed on Internet commerce, while members of Congress adopted the laissez-faire approach to the regulation of the Internet. They were reluctant to impose regulatory controls on website operators, preferring to give the private sector time to develop its own online privacy policies.[5]

Due to the profound effect on global commerce, the Internet poses several unique and complicated legal challenges to American lawmakers. In attempts to confront such Internet-related issues, lawmakers have struggled balancing the different needs and interests of private and public sectors in hopes of reaching some sort of universal harmony in the area of technology and federal regulation. This compilation is a legislative history of the federal law of encryption technology as it made its way to the enactment of the Electronic Signatures in Global and National Commerce Act.

Encryption is the electronic scrambling or coding of computer messages and telecommunication signals for privacy and security purposes. It is a set of complex mathematical formulas that permit anyone transmitting electronic information to scramble the message so that only the intended recipient can decode the message with a secret code. This technology is used to encode information ranging from credit card numbers to national security plans.

There are two types of encryption systems: symmetric key encryption and public key encryption. Symmetric key encryption is the more traditional form of cryptography, by which a single key can be used to encrypt and decrypt a message.[6] The sender and the recipient use the same key to encrypt and decrypt the message, hence the obvious downfall that anyone having access to the sender's key can encode and

---

5. *See id.*

6. David B. Walker, *Privacy in the Digital Age: Encryption Policy – A Call for Congressional Action,* 1999 STAN. TECH. L. REV. 3, 15 (1999).

decode the message.[7] Asymmetric or "public key" cryptography is more appropriate for the typical on-line business transaction. With public key cryptography, the sender (or recipient) has a private key, which is not revealed to anyone.[8] That private key is uniquely matched to a public key that is given to the recipients.[9] The keys are linked in such a manner that the public key will be able to encrypt messages that may only be decrypted by the holder of the private key and vice versa.[10]

Although complex, it must be noted that the use of encryption technology to scramble or unscramble a message is not a digital signature. Encryption technology is however a step in creating a digital signature.[11] Due to its importance in preserving privacy and security, encryption is integrated into many computer networks and World Wide Web browsers. Encryption is also incorporated into chips in personal computers and other electronic devises, such as wireless telephones. It affects almost everything Americans encounter.

This collection includes the agency reports from the Congressional Research Service, the Office of Technology Assessment, and the General Accounting Office. Moreover, it includes various crucial bills on encryption technology as they went through the congressional process; and congressional prints, hearings and reports that indicate Congress' intent and outline their policy considerations. Additionally, provisions of the Federal Register promulgating the rules on encryption are also included. The following article touches the key issues generating the need and process of such technology reform.

The Need for Secrecy in the Digital Age

Secrecy has been a preoccupation of nations and empires for centuries, mainly to keep military communications private. Encryption was initially the exclusive domain of national security agencies, concerned with strict security of the highly potent information they transmit, especially over the Internet. However, encryption has recently become increasingly

---

7. Raneta Lawson Mack, *Digital Signatures, the Electronic Economy and the Protection of National Security: Some Distinctions with an Economic Difference,* 17 J. MARSHALL J. COMPUTER & INFO. L. 981, 986 (1999).

8. *See id.*

9. *Id.*

10. *See id.* at 987

11. Mack, *supra* note 7, at 987.

important to the private sector. With the emergence of e-commerce, encryption has diversified its importance by extending itself to the urgent concerns of ordinary citizens conducting online business transactions.[12] Their concerns are caused by the ease in intercepting or tampering with digital information within the online environment. With the use of encryption, such interception can be precluded. Encryption provides the locks and keys of the information age, and is akin to an envelope in that it prevents eavesdroppers from discovering the contents of a message.[13] To exemplify, in today's day and age, many individuals send credit card information over the Internet, who would not be inclined to do so if they did not think that it was safe. This "safety" is provided by the use of encryption technology. Thus, businesses and consumers want strong encryption products to protect the information they transmit to each other. It is notable that both Internet-based companies and the traditional producers of goods and services are transforming the way they do business into an e-commerce process so as to lower costs, improve customer service, and increase productivity.[14] This trend thereby reiterates the desire and need for encryption.

The Role of Encryption Technology

Although the benefits of encryption to the private sector were abundant, there was concern as to how the law enforcement community would be able to monitor undesirable activity in the digital age. The concern stemmed from lawmakers' inner conflicts between allowing the private sector the opportunity for growth through self-regulation, and the need for protecting consumers and preventing domestic and international crime. Although the Clinton Administration had supported an initial self-regulatory approach, it had warned the industry that failure to implement a strong workable system to protect consumers would trigger legislation mandating privacy protection of such consumers.[15] The problem was that

---

12. Bob Ranking, *Secrets of the Crypt*, NEWSDAY, Oct. 15, 1997, at CO3; *Safe and Secure*, P.C. MAG., May 5, 1998, at 107.

13. Ira S. Rubinstein & Michael Hintze, *Export Controls on Encryption Software*, 812 PLI COMM. 505, 510 (December 2000).

14. *Electronic Commerce: Worldwide Growth of the Digital Economy*, 79 CONG. DIG. 37 (February 2000).

15. *Internet Privacy: Protecting Personal Information Online*, 79 CONG. DIG. 33 (February 2000).

while encryption benefited e-commerce, it also benefited criminal activity and espionage, due to the difficulty in monitoring and convicting criminals whose messages were in fact encrypted, thus raising national security concerns and opposition by the FBI. Congress grew impatient with the pace of industry self regulation. Consequently, in 1998, the 105th Congress enacted two privacy protection laws: the Children's Online Privacy Protection Act, requiring websites to obtain parental consent before collecting personal information from children, and the Theft and Assumption Deterrence Act, a measure that criminalized identity theft using such personal information as credit card and Social Security numbers.[16] Such mechanisms became necessary in order to protect sensitive information transmitted over the Internet, and to protect U.S. consumers from criminal intrusions.

From Domestic Boundaries to the Export Arena: Restricting Encryption Under the Arms Export Control Act

In the U.S., there had traditionally been few restrictions on the manufacture, use or sale of encryption technology for domestic use. However, the federal government had treated exports significantly different. Under the law as it existed in the mid 1990s, the federal government prohibited the export of encryption hardware or software that was readable only with an electronic key feature of more than forty bits, which was relatively weak. The ban originated from the Arms Export Act of 1976 (PL 94-239) which has been interpreted by the State Department's Office of Defense Trade Controls through the implementation of rules known as the International Trade in Arms Regulation (ITAR).[17] ITAR authorized the President of the United States to control the import and export of "defense articles and defense devices."[18] ITAR also identified "military cryptographic (including key management systems), equipment, modules, integrated circuits, components of software with the capability of maintaining secrecy or confidentiality of information or information systems" as munitions

16. *See id.*

17. Mack, *supra* note 7, at 988. *See also*, BERNARD D. REAMS, JR., DOCUMENTS ON U.S. TECHNOLOGY TRANSFER: THE EXPORT ADMINISTRATION ACTS IN THE UNITED STATED, 1969-1985 (1986).

18. *See id.*

subject to licensing requirement.[19] While the law at the time prohibited the sale of more sophisticated packages overseas, the ban successfully stopped major software makers from dedicating significant resources to encryption. In November of 1996, the President transferred jurisdiction over non-military encryption products and related technology from the Department of State to the Department of Commerce.[20] The result placed non-military encryption products on the Commerce Control List and subjected them to the Export Administration Regulations, while military products remained regulated by the ITAR.[21]

One of the most controversial encryption-related concerns was determining how much access the government should have to encrypted stored computer data or electronic communication for the purposes of law enforcement and national security. U.S. law enforcement officials expressed several concerns involving crime prevention and criminal apprehension. They also argued that by protecting criminal communications, strong encryption jeopardized national security. Thus, a controversy emerged between civil libertarians, who wanted unlimited access to strong encryption and law enforcement advocates who wanted to ensure a means of monitoring private communications. All of the regulatory changes eventually favored civil libertarians, largely because they had the support of "big business" on their side.

Not only did American business interests and several lawmakers believe that the U.S. government's export restrictions were unworkable, but they also feared the U.S. was losing ground in a potentially lucrative international high-tech market composed of legitimate businesses and individuals who wanted to prevent unauthorized access to their propriety material. American companies argued that U.S. export policies were hurting their market share while helping foreign companies that were not subject to the same export restrictions. It was not until 1996, that Congress began considering a series of bills regarding these matters in more depth, and in doing so, increased legislative involvement was triggered.

The Clinton Administration strongly supported arguments by law enforcement and national security agencies that urged government access to the plain text encrypted electronic data and messages to investigate

---

19. *Id.*
20. *Id.*
21. *See id.* at 989.

suspected criminal activity. Besides international criminal activity, the Administration (notably the FBI) wanted to even monitor domestic criminal activity with such access. However, the Administration had always permitted use of any strength encryption, without a key recovery requirement, for domestic use, and to mandate otherwise, would bring several Constitutional controversies to fruition. Key recovery is the general term given to the numerous ways to gain "emergency access" to encrypted information.[22] A common key recovery method is key escrow and involves splitting a decryption key, whether secret or public, "into several parts and distributing these parts to escrow agents, or 'trustees.'"[23] Should recovery ever be necessary, these trustees would be able to decrypt the encrypted message or use their "share" of the key to reconstruct the missing key.[24] Based on the potential for access, the Administration sought different approaches to promote voluntary key recovery agents. They carried this out by removing the limits on the strength of encryption products that could be exported if they had key recovery, and urging access of such decryption keys available to authorized federal and state government entities.

This thereby intensified the controversy between the Administration and privacy advocates. While the Administration wanted law enforcement access to keys for encrypted data, the privacy advocates maintained their position that law entities would have too much access to private information. Although many business and consumer groups agreed that key recovery was desirable when keys are lost, stolen, or corrupted, they wanted market forces to drive the development of key recovery encryption products, rather than the government. Opponents of controls insisted that the government should have no role in choosing who holds the keys, otherwise the government would have unfettered access to private files and communications. Once again, another "tug of war" continued.

---

22. D. Forest Wolfe, Comment, *The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption*, 49 EMORY L.J. 711, 716 (2000).

23. *Id.* at 717.

24. Wolfe, *supra* at note 22, at 717.

Bringing It All Together: Encryption and Electronic Signatures

The growth of the Internet has provided unlimited possibilities for businesses and consumers, not only to participate in global electronic commerce transactions, but moreover to develop such e-commerce transactions. Given the potential benefits to merchants and consumers involved in e-commerce, mechanisms are required to ensure that information is transmitted securely and confidentially.[25] The ability to authenticate and verify the participants in an online transaction is imperative. These cumulative concerns bring about the "Electronic Signatures in Global and National Commerce Act," commonly referred to as "E-SIGN." This Act establishes the validity of electronic signatures, and its purpose is to ensure that no signature or contract will be ruled invalid solely because it is in electronic form.[26] Although it replaces the traditional paper method of recording with electronic recording, it still imposes limits. It requires active consent by all parties involved in any on-line transaction in which the consent must be provided electronically.[27]

The Act goes even further to exempt certain classes of transactions from those that are allowable. In other words, there are transactions that may not be conducted by electronic records, notice or signatures, and thus must be conducted on paper. The set of exceptions includes, "wills, divorce, and adoption documents, court orders and other court documents, eviction or foreclosure notices, notice of cancellation of life insurance or health insurance, cancellation of utility services, and product recall notices that impact health or safety."[28]

There are several justifications that supported the enactment of the E-SIGN. To illustrate, over forty-five states already have some kind of legislation establishing the validity of electronic signatures.[29] The states' statutes however create numerous difficulties due to the varying standards for authentication and certification authorities; thus, individuals participating in interstate e-commerce transactions cannot be certain that an electronically signed document will be given the same

---

25. Mack, *supra* note 7, at 985.

26. *See* Bill Zoellick, *Wide Use of Electronic Signatures Awaits Market Decisions About their Risks and Benefits*, 72 N.Y. ST. B.J. 10, 11 (Dec. 2000).

27. *Id.*

28. *Id.*

29. *See id.* at 10.

recognition in every jurisdiction, and further because of the variety of state standards and procedures governing the authenticity and validity of digital signatures.[30] The federal law, thereby provides "a way to harmonize the different state regulations and a framework for interstate commerce."[31] It does so with E-SIGN. Electronic signatures, coupled with encryption, are capable of ensuring the integrity of a message and promoting e-commerce throughout, and with E-SIGN, with more consistency.[32]

These are just some of the many different issues that battled lawmakers in their pursuit for neutral ground in the area of e-commerce. Although the tug of war is not yet over, this compilation encompasses the different policy considerations and challenges that faced Congress. Once embarked on this legislative journey, the understanding of encryption law and its importance in the new millennium will come full circle. As President Clinton stated,

> It will encourage the information technology revolution that has helped lower inflation, raise productivity, and spur new research and development by marrying one of our oldest values—our commitment to consumer protection—with the newest technologies, we can achieve the full measure of the benefits that e-commerce has to offer.[33]

30. Mack, *supra* note 7, at 996.

31. Zoellick, *supra* note 26 at 10.

32. *See id.* at 14.

33. President's Statement on the House of Representatives Action on Electronic Signatures, 36 WEEKLY COMP. OF PRES. DOC 1365 (June 19, 2000).