The John Marshall Journal of Information Technology & Privacy Law

Volume 17
Issue 3 *Journal of Computer & Information Law - Spring 1999*

Article 8

Spring 1999

The Regulation of the Internet Encryption Technologies: Separating the Wheat from the Chaff, 17 J. Marshall J. Computer & Info. L. 945 (1999)

Kurt M. Saunders

THE REGULATION OF INTERNET ENCRYPTION TECHNOLOGIES: SEPARATING THE WHEAT FROM THE CHAFF

by KURT M. SAUNDERS†

"His winnowing fork is in his hand . . . gathering his wheat . . . and burning up the chaff . . . ."[1]

I. INTRODUCTION

Federal efforts to strictly regulate the export of strong digital encryption continue to be outpaced by the realities of technological innovation and diffusion. The widespread use of computers and networks to facilitate personal communications and commercial transactions[2] has moved the need for strong encryption technology to the forefront. Cryptography has a long history as a tool for protecting the secrecy of communications, most typically in the context of military operations.[3] For individuals and businesses, however, its relevance and utility as a means for ensuring security has been underscored with the advent of the information age.

In an effort to stem growing concerns about the integrity and confidentiality of electronic proprietary data and communications, and in order to prevent theft and industrial espionage, many businesses are turning to robust encryption technologies to secure such information while in storage or in transmission. Likewise, many individuals increas-

† Assistant Professor of Business Law, California State University, Northridge. The author wishes to thank Professor Mike Closen and the editors of *The John Marshall Journal of Computer & Information Law* for the opportunity to be part of this symposium.

1. *Matthew* 3:12 (King James).

2. Recent estimates as to the size and projected growth of the digital economy are summarized in U.S. GOV'T WORKING GROUP ON ELEC. COMMERCE ANN. REP. 1-2 (1998); *see also* United States Dept. of Commerce, *The Emerging Digital Economy* (visited Apr. 18, 1998) <http:// www.ecommerce.gov/emerging.htm>.

3. For a concise history of cryptography, see Shireen J. Hebert, *A Brief History of Cryptography* (visited Nov. 11, 1998) <http://www.cybercrimes.net/Cryptography/Articles%20on%20Cryptography/BriefHistCrypt.html>.

ingly use encryption in their private communications to ensure their privacy and to prevent identity fraud.[4]

At the same time, however, the growing use of encryption has led to concerns on the part of federal law enforcement and national security authorities that these technologies will be employed for criminal and terrorist purposes.[5] Indeed, the government believes that the United States is highly vulnerable to attack electronically. To demonstrate this, the Defense Department recently hired a team of computer hackers to discover how far they could penetrate government and critical infrastructure systems, finding that they were able to get surprisingly far in just three months.[6] Nevertheless, current federal restrictions on encryption technologies may, in the long run, critically threaten individual privacy[7] and undermine the position of U.S. businesses in the international market for secure software and on-line commercial transactions.[8]

Indeed, the present encryption regulatory regime is a product of U.S. national security policy and law enforcement strategy. The government has sought to impede the development and diffusion of digital encryption technologies through the use of export controls. As a consequence, the export of cryptography was restricted under the Arms Export Control

4. Identity theft involves the illicit use of another person's identifying facts (e.g., name, birthdate, Social Security number, address, or telephone number) to perpetrate an economic fraud. The personal hardships of the victims and general economic consequences of this misconduct are discussed in *The Prepared Statement of the Federal Trade Commission on "Identity Theft" Before the Subcomm. On Technology, terrorism and Government Information of the Senate Comm. on the Judiciary*, 105th Cong. (1998) (statement of David Medine, Ass'n. Dir. for Credit Practices, Bureau of Consumer Protection, Federal Trade Commission). The recently enacted Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028(a), makes the theft of personal information with the intent to commit an unlawful act a federal crime with penalties of up to fifteen years of imprisonment and a maximum fine of $250,000. The enforcement scheme and likely impact of this statute are more fully considered in Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL J. L. & PUB. POL'Y 20 (1999).

5. *See Impact of Encryption on Law Enforcement and Public Safety: Hearings Before the Senate Comm. on Commerce, Science, and Transportation*, 104th Cong. (1996) (statement of Louis J. Freeh, Dir., Federal Bureau of Investigation). *See also* Report of a Special Panel of the ACM U.S. Public Policy Committee (USACM), *Codes, Keys and Conflicts: Issues in U.S. Crypto Policy*, (visited Dec. 8, 1998) <http:// info.acm.org/REPORTS/ ACM_CRYPTO_STUDY/_WEB/c_report. html>.

6. *See* Michael Stutz, *No 'Right' to Crypto Export*, WIRED NEWS (visited Dec. 4, 1998) <www.wired.com/news/news/technology/story/ 14098.html>.

7. *See infra* text accompanying notes 77-79.

8. The policies of most other countries are more liberal than that of the United States. For a survey of the cryptography policies of over 200 nations and territories around the world, see Wayne Madsen et al., *Cryptography and Liberty: An International Survey of Encryption Policy*, 16 J. MARSHALL J. COMPUTER & INFO. L. 475 (1998).

Act.[9] For a while, most encryption software was also categorized as a munition and its export regulated by the State Department.[10] In December of 1996, control over the export of encryption products was shifted to the purview of the Commerce Department, where they are presently regulated as "encryption items."[11]

Recently, however, Professor Ronald Rivest of the Massachusetts Institute of Technology developed a new method of securing the electronic transmission of data, known as *chaffing and winnowing*,[12] that evades current federal regulation as an encryption item. The method uses electronic *authentication*, rather than encryption, to provide security and maintain confidentiality.[13] Because message authentication codes used with this technology are not considered to be encryption,[14] the chaffing and winnowing method may effectively sidestep existing controls.[15]

This article uses Rivest's method as a point of departure for considering the impracticality of U.S. regulatory policy as applied to digital encryption. As a prelude, I will outline the technology and then discuss the utility of cryptography and the legal framework used to regulate its use and export abroad. Next, I will examine the chaffing and winnowing method of authentication as a means of ensuring secure date transmission that lies outside the reach of current encryption export controls. The article will then conclude with a critique of the government's ongoing attempts to regulate encryption and identify the risks that such efforts pose to individual privacy and the competitive position of U.S. businesses in the global marketplace.

II. THE TECHNOLOGY OF DIGITAL CRYPTOGRAPHY

The basic concept of digital encryption is simple: using a computer program, an encryption algorithm (a mathematical equation) converts a plaintext message and encodes it, using a *key*,[16] into apparently unintel-

9. Arms Export Control Act of 1976, Pub. L. No. 94-329, title II, § 212(a)(1), 90 Stat. 744 (1976) (codified at 22 U.S.C. § 2778 (1994)) (repealing the Mutual Security Act, ch. 937, 68 Stat. 832 (1954)).

10. *See infra* text accompanying note 31.

11. *See infra* text accompanying note 32.

12. Ronald L. Rivest, *Chaffing and Winnowing: Confidentiality without Encryption* (visited Nov. 11, 1998) <http://theory.lcs.mit.edu/ ~rivest/chaffing.txt> [hereinafter Rivest].

13. *See infra* text accompanying notes 61-63.

14. *See infra* text accompanying note 35.

15. Charles Platt, *Encryption*, WIRED, July, 1998, at 76 ("Rivest's idea offers the best of both worlds: confidentiality and adherence to the law—while making a mockery of the latter in the process."); Anne Eisenberg, *Confidentially Yours*, SCIENTIFIC AMERICAN, June, 1998, at 21 ("[Rivest's] new technique to send confidential messages may finally scotch government policies restricting the export of encryption technology.").

16. The length of a key is measured in *bits*, the digits "0" and "1" used to encode computer data. The greater the number of bits, the more secure is the key.

ligible ciphertext.[17] Consider a simple example where the message "Excelsior!" is encrypted using a key that shifts the letters of each word by one:

EXCELSIOR! ⇒ FYDFMTJPS!

The level of difficulty a third party would have in "breaking the code" determines the strength of a key and the robustness of the encryption system. Typically, the longer the mathematical algorithm employed, the more secure the encryption system.

There are two basic and widely available types of encryption systems: private key and public key encryption. In a *private key* encryption system,[18] the key used to encode the information is sent to the recipient, who uses it to decode the encrypted message. The principal drawback to a private key encryption is the risk incurred in sending the key to the intended recipient. Key management is essential; the sender and recipient must use another, secure channel, or protocol, to agree on and exchange a common key. The level of security in this system is correlative of the security of the key's delivery.[19]

In a *public key* encryption system,[20] by contrast, there are two mathematically related keys: a private key and a public key. Using a private key, one can encode a message that can only be decrypted with that person's public key. Alternatively, the person can use the recipient's public key to encrypt a message, which can only be decoded with the recipient's private key and no other. The risk to key security is thereby reduced.[21]

Public key encryption can also be used to generate a *digital signature*, which can be used to authenticate the identity of a sender of a message as well as its contents.[22] A digital signature functions as a ver-

17. *See* STIMSON GARFINKLE & GENE SPAFFORD, WEB SECURITY AND COMMERCE 187-208 (1997). For excellent online sources of information about cryptographic terminology, methods, and software, see *Cryptography A-2-Z* (visited Dec. 4, 1998) <http://www.ssh.fi/tech/crypto/>; Paul Fahn, *Answers to Frequently Asked Questions About Today's Cryptography* (visited Apr. 18, 1998) <http://www.rsa.com/rsalabs/newfaq/>.

18. Private key systems are sometimes referred to as "secret key" or "symmetric" key systems.

19. Nonetheless, prudent key management requires that keys be retired and replaced at periodic intervals to prevent intruders from using exemplars of ciphertext to break the key. GARFINKLE & SPAFFORD, *supra* note 17, at 187-208.

20. Public key systems are also referred to as "dual key" or "asymmetric" key systems.

21. Key management remains an issue, however, in that the message sender's private key must remain confidential to avoid unauthorized use. In addition, ensuring that the public key really belongs to the sender requires the involvement of a certification authority—a reliable third party that associates a public key with a particular individual. *See* Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce,* 75 OR. L. REV. 49, 55-56 (1996).

22. In on-line commercial transactions, the authentication of identity and mutual assent is a foundational issue. *See* Jane K. Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce,* 72 TUL. L. REV. 1177 (1998) (addressing the controversy over

ification "seal" that the message has not been modified without the sender's authorization.[23]

In order to create a digital signature, a message digest, or *hash*, representing the text of the message must be first be created by running the contents of the message through a hash function that yields a unique value. This value is unique to the message in that any subsequent change in the message text will yield a different value. A digital signature is produced by using the sender's private key to encrypt the hash, and the encrypted hash is then sent with the message to the recipient, who can runs the message through the same hash function to produce a second, separate hash. The recipient then decrypts the sender's hash using the sender's public key and compares it to the second hash; if the two hashes are identical, the authenticity of the message is verified.[24]

Steganography is yet another cryptographic method that digitally encodes or embeds one piece of information within another.[25] Digitized visual or audio files usually contain unused or insignificant areas of data. Steganography replaces these areas with indelible information without otherwise degrading or altering the quality of the file. The file can then be transmitted without detection. Thus, a digitized recording or image might contain a private message. Sometimes referred to as "digital watermarking" or "digital fingerprinting," steganography has been used to place a hidden copyright or trademark tag in images posted online.[26]

III. THE REGULATION OF DIGITAL CRYPTOGRAPHY

At the present time, there are no restrictions on the manufacture, sale, or use of encryption technologies within the United States. Likewise, there are no restrictions on the import of encryption technologies into the United States. The export of encryption, however, is governed by

---

authentication procedures used in Internet business transactions); Matthew D. Ford, *Identity Authentication and 'E-Commerce,'* 1998(3) J. INFO., L. & TECH. <http://www.law.warwick.ac.uk/jilt/98-3/ford.html> (analyzing various identity authentication systems and authority authentication).

23. Intellectual Property and the National Information Infrastructure, THE REP. OF THE WORKING GROUP ON INTELL. PROP. RTS. 188 (1995) [hereinafter IP AND THE NII].

24. Digital signatures will play an important role in Article 2B of the Uniform Commercial Code when it is eventually completed. As well, many states are in the process of enacting laws concerning the use of digital signatures. For a current summary of such legislation, see McBride, Baker & Coles, *Summary of Electronic Commerce and Digital Signature Legislation* (visited April 18, 1998) <http://www.mbc.com/ ds_sum.html>.

25. For detailed information about steganography, see the Steganography Info & Archive (visited Dec. 3, 1998) <http://members.iquest.net/ ~mrmil/stego.html>; *see also* Fabien A. P. Petitcolas, *On the Limits of Steganography* (visited Feb. 1, 1999) <http://www.cl.cam.ac.uk/~fapp2/papers/jsac98-1/node2.html>.

26. IP AND THE NII, *supra* note 23, at 189.

the Arms Export Control Act (AECA),[27] which is administered by the State Department under the International Traffic in Arms Regulations (ITAR),[28] and the Export Administration Act (EAA),[29] along with the Export Administration Regulations (EAR),[30] which are administered by the Commerce Department.

Digital cryptography is treated as a dual use technology. Dual use technologies are those that have both military and civilian use. Many encryption technologies were once defined as "munitions" and their export prohibited under the EAR, but in 1996, encryption technologies were transferred from the Munitions List of the AECA to the Commerce Control List under the EAA.[31] Presently, the Commerce Department regulates all encryption technologies, except those developed exclusively for the use of the military.

In general, a license is required for the export of "encryption items," which include all encryption commodities, software, and technology that contain encryption features and are subject to the EAR.[32] The "export" of controlled items includes encrytion source code and is defined as "downloading, or causing the downloading of, such software to locations. . .outside of the United States. . . ."[33] Some types of encryption items are exempted, including access control equipment, such as automatic teller machines, self-service statement printers or point of sale terminals, that protects password or personal identification numbers to prevent unauthorized access; and cryptographic equipment specially designed and limited for use in banking or money transactions.[34] Also exempted is data authentication equipment that calculates a message authentication code (MAC) or similar result to ensure no alteration of text has taken place or to authenticate users.[35]

Federal efforts to regulate encryption have not been limited to restrictions on exports. In 1995, for example, the government launched the so-called "Clipper Chip" initiative in an attempt to establish an encryption standard accessible to law enforcement authorities by court order. The stated purpose of the initiative was to allow the government to thwart terrorism, drug trafficking, foreign espionage, and other crimes that might make use of encryption technology to evade surveillance and detection. Under this initiative, all electronic encryption technology was

27. 22 U.S.C. § 2778 (1994).
28. 22 C.F.R. § 120 (1993).
29. 50 U.S.C. § 2401-2420 (1994).
30. 15 C.F.R. § 730-799 (1996).
31. *See* Exec. Order No. 13,026, 61 Fed. Reg. 58,767, 68,572 (1996).
32. 15 C.F.R. § 734.1 (1996).
33. *Id.* § 734.2(b)(9).
34. *Id.* § 734.2.
35. *Id.*

to be subject to key escrow whereby the government would hold a copy of the keys used for encrypting and decrypting messages. However, the Clipper Chip initiative provoked such a firestorm of protest on constitutional and economic grounds that it was soon abandoned.[36]

There have also been several challenges to the federal government's encryption export regulations. In *Bernstein v. United States Dep't of State,*[37] the court was presented with the issue of whether the federal export controls on the publication of encryption software source code amounted to a unconstitutional restraint on free speech.[38] Daniel Bernstein, a graduate student at the University of California at Berkeley, wrote an encryption program that he named "Snuffle." He wanted to post Snuffle on the Internet for use by other students[39] and submitted a commodity jurisdiction request to the Department of State to determine whether the program was subject to government regulation.[40] When the State Department denied him permission to distribute the program,[41] Bernstein sued, claiming that his First Amendment right of free speech had been violated.[42]

The federal district court held that the Snuffle program's source code[43] was speech under the First Amendment and that the govern-

36. *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

37. Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (N.D. Cal.) (denying motion to dismiss), *partial summary judgment granted,* 945 F. Supp. 1279 (1996), *superseded,* 974 F. Supp. 1288 (1997).

38. For an extended analysis and critique of this decision, see Patrick I. Ross, *Computer Programming Language*: Bernstein v. United States Department of State, 13 BERKELEY TECH. L. J. 405 (1998) (concluding that whether computer source code is constitutionally protected free speech and whether export controls on cryptography are unconstitutional requires a detailed factual analysis). For other discussions of the First Amendment protection of encryption issue, see E. John Park, *Protecting the Core Values of the First Amendment in an Age of New Technologies: Scientific Expression vs. National Security,* 2 VA. J.L. & TECH. 3 (1997); Jan H. Samoriski, et al., *Encryption and the First Amendment,* 2 COMM. L. & POL'Y (1997); Phillip E. Reiman, Comment, *Cryptography and the First Amendment: The Right to Be Unheard,* 14 J. MARSHALL J. COMPUTER & INFO. L. 325 (1996); Elizabeth Lauzon, Note, *The Philip Zimmermann Investigation: The Start of the Fall of Export Restrictions on Encryption Software under First Amendment Free Speech Issues,* 48 SYRACUSE L. REV. 1307 (1998).

39. 945 F. Supp. at 1289-90.

40. *Id.* at 1296.

41. *Id.*

42. Bernstein had also submitted commodity jurisdiction requests for several written texts that contained the Snuffle algorithm and description. Initially, the State Department denied him permission to distribute the texts, but retracted this decision after Bernstein filed suit. Bernstein v. Dep't of State, 922 F. Supp. at 1433-34.

43. Source code is "the series of instructions to the computer for carrying out the various tasks which are performed by the program, expressed in a programming language which is easily comprehensible to appropriately trained human beings." SAS Inst., Inc. v. S & H Computer Sys., 605 F. Supp. 816, 818 (M.D. Tenn. 1985).

ment's licensing scheme was an illegal prior restraint on speech.[44] In reaching this conclusion, the court reasoned that source code was "language" in that it is "the expression of ideas, commands [and] objectives"[45] and that even though Snuffle may have been "essentially functional, that does not remove it from the realm of speech."[46]

Another challenge to the federal export controls arose in *Karn v. United States Dep't of State.*[47] In 1996, Philip Karn filed suit challenging the State Department's denial of permission to export a diskette containing the source code for several encryption algorithms printed in the book *Applied Cryptography* by Bruce Schneier.[48] The State Department approved the export of the book itself, but not the diskette containing identical information. Karn sought review in federal district court of the government's denial claiming that the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) were unconstitutional under the First and Fifth Amendments.

Though finding, as in *Berstein*, that encryption source code was speech,[49] the court rejected Karn's claims and upheld the constitutionality of the AECA and ITAR on the grounds that they furthered an important or substantial governmental interest.[50] In addition, the court rejected his argument that the ITAR constituted a prior restraint on free speech since the regulations were content-neutral.[51] Karn then appealed, but on December 30, 1996, just before oral arguments were to be heard, the President transferred the responsibility for export regulation of civilian encryption software from the State Department to the Commerce Department.[52] Accordingly, the court of appeals remanded the case to the district court for review under the Commerce Department's new Export Administration Regulations (EAR).

More recently, in the case of *Junger v. Daly,*[53] Professor Peter Junger filed suit to establish that it is within his First Amendment right to teach his "Computers and the Law" class online at Case Western Reserve University School of Law and to post encryption software on his Web site. Junger sought relief for himself as well as a permanent injunction enjoining the government from enforcing the encryption software

44. 945 F. Supp. at 1289.
45. 922 F. Supp. at 1435.
46. *Id.*
47. 925 F. Supp. 1 (D.D.C. 1996), *remanded,* 107 F.3d 923 (D.C. Cir. 1997).
48. BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY (2d ed. 1996).
49. 925 F. Supp. at 12.
50. *Id.* at 6.
51. *Id.* at 9-12.
52. *See supra* text accompanying note 31.
53. Junger v. Daly, 8 F. Supp. 2d. 708 (N.D. Ohio 1998). For additional information regarding this case, *see Free Speech and the Export of Crypto* (visited Nov. 5, 1998) <http://samsara.law.cwru.edu/comp_law/crypto_export/>.

and technology provisions of EAR against anyone who seeks to disclose or export encryption technology.[54]

In a decision that puts it at odds with that in *Bernstein*,[55] the court granted summary judgment in favor of the government, holding that the export of encryption source code on the Internet was not protected by the First Amendment.[56] Specifically, the court held that the EAR "are constitutional because encryption source code is inherently functional, because the Export Regulations are not directed at source code's expressive elements, and because the Export Regulations do not reach academic discussions of software, or software in print form."[57]

The court's decision stands in contradiction with the *Bernstein* holding by ruling that the EAR is content neutral because it controls the *functionality* of the program rather than its *content*.[58] This is a false dichotomy, however, in that a change in the function of a program requires a change to the content of its source code as well.[59] Nevertheless, given the nature of these issues and the debate surrounding the future of encryption export restrictions, neither the *Junger* and *Karn* cases nor the decision in *Bernstein* are likely to represent the last word on this matter.

IV. CONFIDENTIALITY THROUGH "CHAFFING AND WINNOWING"

In 1977, Ronald Rivest, along with Adi Shamir and Leonard M. Adleman, published and later distributed their encryption algorithm known as RSA, which became the standard in public key cryptography and which is widely used for digital signatures.[60] In March of 1998, Rivest proposed a new method for secure data transmission over the Internet that he has labeled as *chaffing and winnowing*.

Using this method, messages are sent electronically in a combination of "good" packets (wheat) and "bad" packets (chaff). There are two steps to sending a message; authenticating and adding chaff. The recipient removes the chaff to obtain the original message. Thus, the sender first breaks the message into packets, and authenticates by appending to

54. *Id.* at 711-12.

55. Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (pending before the Ninth Circuit).

56. The reasoning was consistent with that of the court in *Karn*, at least as to the prior restraint issue. *See id.* at 718-19.

57. *Id.* at 712.

58. *Id.* at 721-23.

59. The question of whether the source code is expressive or merely functional is reminiscent of the debate surrounding the issue of whether source code is copyrightable. *See* RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY ¶ 1.04 (rev. ed. 1992).

60. *See* Hebert, *supra* note 3, at 2.

each packet a message authentication code (MAC) computed as a function of the packet contents and a secret authentication key:

PACKET ⇒ PACKET + MAC[61]

There has been no encryption performed because software that merely authenticates messages by adding MACs[62] is approved for export as it is deemed not to encrypt.[63] A private key shared by the sender and the recipient to authenticate the origin and contents of each packet allows the recipient to determine that a packet is authentic by recomputing the MAC and comparing it to that received appended to the packet. If the comparison fails, the packet and its MAC are automatically discarded.[64]

Each packet also contains a unique serial number allowing the receiver to remove duplicate packets, identify missing packets, and to correctly order the received packets when reassembling the file. The MAC for a packet is computed as a function of the serial number of the packet as well as of the packet contents and the private authentication key.[65] Consider a simple example, arranged by sequence number, message, and MAC:

1 - Hi Bob + (465231)

2 - Meet me at + (782290)

3 - 7PM + (344287)

4 - Love, Alice + (312265)[66]

The second step involves adding chaff—"fake packets with bogus MACs."[67] The chaff packets have the correct overall format, have reasonable serial numbers, and reasonable message contents, but they have invalid MACs. It will be best to add at least one chaff packet for each packet serial number used by the message. Creating chaff is accomplished by creating fake packets with bogus randomly guessed (and therefore invalid) MACs; to randomly guess a MAC requires no knowledge of the private authentication key. The chaff packets are then randomly intermingled with the good (wheat) packets to form the transmitted packet sequence. The chaff packets might make the received sequence in our example appear as follows:

1 - Hi Larry, + (532105)

1 - Hi Bob, + (465231)

---

61. Rivest, *supra* note 12, at 1.

62. The use of MACs can be replaced by the type of digital signatures that allow the user to designate the verifier. *Id.* at 6.

63. *See supra* text accompanying note 34.

64. Rivest, *supra* note 12, at 2.

65. *Id.*

66. *Id.*

67. *Id.*

2 - Meet me at + (782290)
2 - I'll call you at + (793122)
3 - 6PM + (891231)
3 - 7PM + (344287)
4 - Yours, Susan + (553419)
4 - Love, Alice + (312265)[68]

In this example, for each serial number, one packet is good (wheat) and one is bad (chaff). A third party, not knowing the private authentication key, cannot distinguish a good (wheat) packet from a bad (chaff) one. Moreover, instead of randomly intermingling the chaff with the wheat, the packets can be output in sorted order, sorting first by serial number, and then by message contents. To obtain the correct message, the recipient merely discards all of the chaff packets, and retains the wheat packets. Smaller packets can provide greater degree of confidentiality.[69] Consider for instance a sequence of packets that are only one letter in length:

1 - H + (74522)
1 - G + (85843)
1 - D + (66344)
2 - E + (90872)
2 - I + (89310)
2 - F + (90086)
3 - A + (21876)
3 - K + (24442)
3 - B + (32451)
4 - R + (53620)
4 - M + (92569)
4 - O + (32316)
5 - B + (24550)
5 - U + (14539)
5 - B + (77531)

After winnowing out the chaff packets using the authentication key, the following message is revealed:

HI BOB

Again, nothing has been encrypted; in fact, the entire message remains clearly visible and even greater security can be had if the method was applied one *bit* at a time.[70] This is due to the fact that Rivest's

68. *Id.*
69. Rivest, *supra* note 12, at 3.
70. If each packet contains a single bit (a single "0" or "1"), the task of breaking the MAC algorithm or the authentication key is virtually impossible. *Id.* This is not to imply,

method uses basic authentication to achieve confidentiality, as he has explained through analogy:

> [an] example of using authentication to achieve confidentiality occurs in baseball—a coach will signal to a runner by giving a sequence of signals, but the real signal is the one immediately following a previously agreed-upon authenticator signal. [Another] example of using authentication to achieve confidentiality occurs in the Rex Stout's novel "The Doorbell Rang." Two men wish to communicate privately, but fear that the FBI has bugged the room. They agree when the speaker raises a finger, his statements are to be disregarded. Of course, the FBI's bugs can't tell if the speaker has his finger raised or lowered![71]

Chaffing and winnowing bear some relationship to steganography. With chaffing and winnowing, a third party may know (or suspect) that there are two different kinds of packets, but the third party will be unable to distinguish them because he or she does not possess the secret authentication key.[72] Chaffing and winnowing also bear some resemblance to encryption.

Indeed, the process of authenticating packets and then adding chaff achieves confidentiality, and so qualifies as encryption by anyone who uses a definition of encryption that is so broad as to include all techniques for achieving confidentiality. But this fails to note the special structure here, wherein a non-encrypting key-dependent first step (adding authentication) followed by a non-encrypting keyless second step (adding chaff) achieves confidentiality. Since the second step can be performed by anyone and since the first step (adding authentication) may be performed for other good reasons, we see something novel, where strong confidentiality can even be obtained without the knowledge and permission of the original sender.[73]

The level of confidentiality provided depends on several factors, including the MAC algorithm, how the original message is broken into packets, and how the chaffing is done.[74] A typical MAC algorithm will appear to act like a "random function" to a third party, and in such a case the third party will not be able to distinguish wheat from chaff.[75] As

---

however, that the process is made any less secure by including more bits per packet or by using larger packets authenticated with a robust MAC algorithm. *Id.* at 5.

71. *Id.* at 7.

72. *Id.* at 6. Rivest explains the distinction with steganography by way of an example:

> I am reminded of the steganographic technique of sending an innocuous-looking letter whose letters are written in two different, but very similar fonts. By erasing all letters in one font, the hidden message written in the other font, remains. For this technique(as with most steganographic techniques), security rests on the assumption that the adversary will not notice the use of two fonts.

Id.

73. *Id.*

74. Rivest, *supra* note 12, at 2.

75. *Id.* at 3.

such, the ability to provide confidentiality by chaffing and winnowing is based on the difficulty for the third party in distinguishing the chaff from the wheat and not on the difficulty of breaking an encryption scheme, because there is no encryption performed. For this reason, Rivest's method effectively achieves an end run around federal export controls on encryption.

V. CONCLUSION

Encryption ensures the confidentiality of electronic communications and data, which may be at risk of theft, misuse, or alteration. As Rivest has pointed out, "[t]rying to regulate confidentiality by regulating encryption closes one door and leaves two open (steganography and winnowing)."[76] Any policy that requires recovery of encryption keys would also need to require recovery of authentication keys. Rivest has used a clever analogy to rebut the government's law enforcement and national security justification for key recovery:

> [A]ny U.S. citizen can freely buy a pair of gloves, even though a burglar might use them to ransack a house without leaving fingerprints . . . . Cryptography is a data-protection technology just as gloves are a hand-protection technology. Cryptography protects data from hackers, corporate spies and con artists, whereas gloves protect hands from cuts, scrapes, heat, cold and infection. The former can frustrate FBI wiretapping, and the latter can thwart FBI fingerprint analysis . . . . To get an idea of the intrusiveness and impracticality of key recovery, imagine that whenever you bought a pair of gloves you were legally required to sew latex copies of your fingerprints into the gloves' fingertips![77]

To regulate the chaffing and winnowing method, the U.S. government would need to gain access to all authentication keys.[78] Doing this, however, could greatly increase the risk of economic and identity fraud, while undermining the privacy of our information infrastructure[79] and

---

76. *Id.* at 1.

77. Ronald L. Rivest, *The Case against Regulating Encryption Technology*, SCIENTIFIC AMERICAN, Oct., 1998, at 116-17.

78. Regarding this possibility, Rivest argues:

> [A]ccess to authentication keys is one thing that government has long agreed that they don't want to have. Having such access would allow the government to forge authentic-looking packets for any pair of parties that are communicating. This is way beyond mere access to encrypted communications, as loss of such authentication keys could wreak massive havoc to the structure and integrity of the entire Internet, allow hackers not only to overhear private messages, but to actually control computers, perhaps to shutdown power systems or to airline traffic control systems, etc. The power to authenticate is in many cases the power to control, and handing all authentication power to the government is beyond all reason, even if it were for well-motivated law-enforcement reasons; the security risks would be totally unacceptable.

Id. at 5.

79. Indeed, the government's ongoing interest in key recovery raises relevant Fourth Amendment search and seizure considerations regarding personal privacy. *See, e.g.*, Anjali

putting at risk the competitive position of the U.S. encryption manufacturers in the global information infrastructure.[80]

Networks such as the Internet are a principal means of distributing software to the mass market. Although strong encryption software can be used and distributed without a license within the United States, networks such as the Internet are readily accessible by those outside of the country. Consequently, any manufacturer that would make encryption technology available on the Internet will immediately encounter the same problem posed in the *Junger* case.[81]

Moreover, despite the export controls, many foreign countries have already obtained and continue to manufacture strong encryption. Indeed, since encryption algorithms such as RSA and others are widely available, any foreign country can easily develop encryption. This demonstrates that U.S. export policy is failing to meet its centerpiece objective. Moreover, imposing key escrow or key recovery as a precondition to relaxing present restrictions ignores the reality that there is little to no market demand for key recovery cryptography when non-key recovery cryptography is readily available elsewhere. This would further undermine the competitive position of American cryptography manufacturers.[82]

Furthermore, such a policy would mark the United States as a site where communications are less secure.[83] This was underscored when, in 1998, the Electronic Frontier Foundation ("EFF") proved that the government's Data Encryption Standard ("DES")—the official federal encryption standard created to protect unclassified computer data and communications uses 56-bit "keys," which is exportable without key recovery—was inadequate and insecure. The EFF sponsored a project that cracked the DES in only three days.[84] Meanwhile, the pace of technological innovation itself has made obsolete the DES in that significantly

---

Singhal, *The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography*, 7 STAN. L. & POL'Y REV. 189 (1996); Kenneth P. Weinberg, Note, *Key Recovery Shaping Cyberspace (Pragmatism and Theory)*, 5 J. INTELL. PROP. L. 667 (1998).

80. Current encryption regulatory policy's detrimental effects on business has been variously discussed. *See, e.g.*, Doug Masson, *The Genie Let Loose: Ineffectual Encryption Export Restrictions and their Deleterious Effect on Business*, 2 J. TECH. L. & POL'Y 3 (1996).

81. *See supra* text accompanying notes 53-59.

82. *See* U.S. Dep't of Commerce & Nat'l. Sec. Agency, *A Study of the International Market for Computer Software with Encryption* (visited Dec. 9, 1998) <http://www.epic.org/crypto/export_controls/ commerce_study_summary.html>.

83. For instance, a hacker who gained access to a key escrow database could seriously undermine security and privacy. This concern and others are summarized in Hal Abelson et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption* (visited Dec. 8, 1998) <http://www.crypto.com/key_study/report.shtml>.

84. *See EFF Builds DES Cracker that Proves that Data Encryption Standard is Insecure* (visited Dec. 5, 1998) <http://www.eff.org/pub/Privacy/ Crypto_misc/DESCracker/>.

stronger 128-bit encryption software is now available and in use.[85]

If the United States stands like a rock in the middle of the information stream, then the flow of encryption technology diffusion and electronic commerce will simply reroute around it. The U.S. government, though, has lately pursued a different strategy with some success. In December of 1998, the Clinton Administration persuaded the thirty-three nations that have signed the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies,[86] to apply the same strict export controls on encryption software as they apply to weapons.[87] Under this agreement, Wassenaar participants would restrict exports of general encryption products using more than 56-bit keys, but allow firms making commercial software for the mass market, such as Internet browsers or electronic mail programs, to use up to 64-bit keys.[88] The agreement imposes no restraints on encryption used to protect entertainment products, such as video transmissions on the Internet, from piracy.[89]

The new agreement may bring the international encryption regulatory scheme more in line with that of the United States.[90] Although there may well be great differences in how effectively the participants enforce the agreement, if nothing else, it might allow U.S. businesses to better compete with foreign software firms. Similarly, it would be foolhardy to believe that those who want strong cryptography for illegal or illicit purposes will be unable to find it, or that methods like chaffing and winnowing will not be utilized lawfully in order to ensure confidentiality. Inevitably, therefore, national security and law enforcement authorities will be compelled to separate their impractical desires from the technological realities of the information age.

---

85. Though it will surely not be the last word on encryption, the 128-bit IDEA algorithm is considered to be highly secure. *See* James. L. Massey & Xuejia Lai, *Device for the Conversion of a Digital Block and the Use of the Same* (May 16, 1991)(patent 5,214,703)(on file with the Patent & Trademark Office), available on LEXIS, Patent Library, Utitlity Design and Plant Patent File.

86. The Wassenaar Arrangement is intended to prevent, through cooperation among the participants, the acquisition and proliferation of armaments and sensitive dual-use technologies for military end uses. The text of the agreement as well as related materials are available on-line at <http://www.wassenaar.org/>. *See also Crypto Setback in Vienna*, WIRED NEWS, Dec. 3, 1998 (visited Dec. 3, 1998) <www.wired.com/news/ news/politics/story/ 16623.html>.

87. The Clinton Administration's approach to this has given a new twist to the old adage, "if you can't beat them, join them;" instead, the strategy appears to have been, "if you won't join them, get them to join you."

88. 15 C.F.R. § 734 (1996).

89. *Id.*

90. *See supra* note 7.