UIC John Marshall Journal of Information Technology & Privacy Law

Volume 14
Issue 2 *Journal of Computer & Information Law - Winter 1996*

Article 6

Winter 1996

Cryptography and the First Amendment: The Right to be Unheard, 14 J. Marshall J. Computer & Info. L. 325 (1996)

Phillip E. Reiman

CRYPTOGRAPHY AND THE FIRST AMENDMENT: THE RIGHT TO BE UNHEARD

I. INTRODUCTION

We are familiar with the reduction in our freedoms accompanying most technological innovations. Metal-detectors search us at the airport; theft-sensors frisk us in the shopping mall and pagers tap us anytime day or night.[1] In the age of lightning-fast computer searches, global networks and wireless communication, our most private information lies exposed to the world.[2] Cryptography, the process of using secret codes to protect or conceal information, dramatically increases our privacy[3] and holds the key to maintaining effective control over an ever-increasing flow of data.[4]

Although historically used by governments to wage war,[5] cryptography can limit access to information, screen electronic communications and provide reliable identification on electronic networks.[6] Services like pay-per-view television and remote banking depend on cryptography.[7]

---

1. Robert Lee Hotz, *Demanding the Ability to Snoop*, LOS ANGELES TIMES, Oct. 3, 1993, at B1.

2. Steven Winters, Comment, *The New Privacy Interest: Electronic Mail in the Workplace*, 8 HIGH TECH. L.J. 197, 219 (1993) (citing Erwin Chemerinsky, *The Supreme Court, 1988 Term-Foreword: The Vanishing Constitution*, 103 HARV. L. REV. 43, 96-98 (1989)). In a recent Defense Department program, experts attacked 12,000 computer systems and succeeded in penetrating security 88% of the time. *U.S. to Propose Federal Agency to Secure Information Superhighway*, WALL ST. J., June 14, 1995, at B9. The attacks went undetected 96% of the time. *Id.*

3. John Mintz & John Schwartz, *Chipping Away at Privacy? Encryption Device Widens Debate Over Rights of U.S. to Eavesdrop*, WASH. POST, May 30, 1993, at C1. Massachusetts representative Edward J. Markey expresses the feelings, "[i]n a digitally linked world, where encryption is the key to privacy, banning encryption may be like banning privacy." *Id.*

4. Timothy B. Lennon, Comment, *The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 be Like 1984?*, 58 ALB. L. REV. 467-71 (1994).

5. DAVID KAHN, THE CODEBREAKERS 190 (1967) (marking the application of the telegraph to battlefield communication in 1844 as the start of modern cryptography).

6. Shimson Berkovits, *Cryptography*, ENCYCLOPEDIA OF PHYSICAL SCIENCE AND TECHNOLOGY, 3 CO-CRYP 849 (Robert A. Meyers ed., 1987).

7. Hotz, *supra* note 1, at B1. On the other hand, the current electronic cash system uses a dangerously weak form of cryptography. *Don't Tell it to the Spartans (Nor, Indeed,*

Control over our personal information is essential in a free society.[8] However, the thought of individual citizens exercising complete command over their own privacy alarms the government.[9] Louis Freeh, director of the Federal Bureau of Investigation, worries about "too much privacy in the wrong hands"[10] and the National Security Agency's General Counsel declares "citizens do not have a constitutional right to unbreakable encryption algorithms."[11] This Comment proposes that current technology has made cryptography a necessary element in maintaining our constitutional right to free speech.[12] Like the printing press,

---

to Anyone Else), THE ECONOMIST, Feb. 18, 1995, at 82. Making an ominous prediction about the digital economy:

> [B]illions of dollars flow across the net each day . . . . [O]rganized crime hires the best hackers. Eventually someone breaks into the system, gaining the ability to coin fake e-cash. He and his colleagues use it widely, surreptitiously to earn a lot of real money . . . . Others notice the system has been breached and the whole world comes tumbling down.

Id.

Sooner than expected, the nightmare came true. William M. Carley & Timothy L. O'Brien, *Cyber Caper: How Citicorp System was Raided and Funds Moved Around the World*, WALL ST. J., Sept. 12, 1995, at A1. A Russian biology student penetrated Citicorp's $500 billion-dollar-a-day network and started siphoning money. *Id.* The intruder moved 12 million dollars and withdrew about $400,000 in cash before being caught, all in a system experts believed was impregnable. *Id.* at A16.

8. Justice Douglas foreshadowed the current crisis in his dissenting opinion in *Osborn v. United States*, 385 U.S. 323 (1966) (Douglas, J., dissenting).

> We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government. The aggressive breaches of privacy by the Government increase by geometric proportions. Wiretapping and 'bugging' run rampant, without effective judicial or legislative control. . . . The dossiers on all citizens mount in number and in size. Now they are being put on computers so that by pressing a button all the miserable, the sick, the suspect, the unpopular, the offbeat people of the Nation can be instantly identified. . . . These examples and many others demonstrate an alarming trend whereby the privacy and dignity of our citizens is being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen—a society in which government may intrude into the secret regions of a man's life at will.

Id. at 341-43.

9. Howard Reingold, *Big Brother Could be Logging On*, SAN FRANCISCO EXAMINER, Apr. 27, 1994, at C2. The American government has had a long involvement with cryptography. When Aaron Burr was tried for treason before Chief Justice John Marshall, one key piece of evidence was a coded letter sent by Burr to his military accomplice, General James Wilkinson. KAHN, *supra* note 5, at 186-87. Another turncoat, Benedict Arnold, sent messages in a code based on Blackstone's *Commentaries*. *Id.* at 177. When Thomas Jefferson served as America's first Secretary of State, he created a code which was secure enough to be used by the United States Navy for almost two hundred years. *Id.* at 192-94.

10. Reingold, *supra* note 9.

11. G. Burgess Allison, *Technology Update*, LAW PRACT. MGMT., Oct. 1994, at 12.

12. The speech component of privacy essentially:

cryptography promises to change the way we think about the exchange of ideas.[13]

The magnitude of this change coupled with a lack of understanding has led to calls for regulation of private cryptography.[14] There are two equally misconceived arguments for the regulation of cryptography.[15] First, cryptography is not speech and therefore, not constitutionally protected at all.[16] Alternatively, cryptography is speech, but the rules of free speech do not apply to cryptography.[17]

This Comment shows that cryptography is undeniably a form of speech. Moreover, it argues that the failure of traditional analysis to effectively categorize cryptography is evidence that it is not simply an extension of existing free speech concepts, but a new dimension to our constitutional rights. Finally, this Comment proposes that like the traditional press, the solution to the question of cryptography regulation lies within the marketplace.[18]

II. BACKGROUND

The concept of a free press is arguably the inevitable consequence of the uncontrolled spread of printing technology.[19] The introduction of printing in England in 1476 led immediately to government licensing of

---

> [P]rovides the individual with the opportunities he needs for sharing confidences and intimacies with those he trusts—spouse, 'family,' personal friends, and close associates at work. The individual discloses because he knows that his confidences will be held, and because he knows that breach of confidence violates social norms in a civilized society . . . .

ALAN F. WESTIN, PRIVACY AND FREEDOM 33-38 (1967).

13. THOMAS L. TEDFORD, FREEDOM OF SPEECH IN THE UNITED STATES 13-16, 322 (2d ed. 1993).

14. Hotz, *supra* note 1, at B1.

15. Traditional First Amendment law does not fit cryptography. When faced with such a situation, the analysis could declare the example a monster and place it outside the definition of speech. LAURENCE H. TRIBE & MICHAEL C. DORF, ON READING THE CONSTITUTION 87-91 (1991). As an alternative, analysis could hold cryptography to be speech, but that it is a special case since so few rules apply. *Id.* A better solution would be to recognize that our definition of speech improperly excludes coded data and that it should adjust to this new definition. *Id.*

16. *Id.*

17. Hotz, *supra* note 1, at B1.

18. Duncan M. Davidson, *Common Law, Uncommon Software*, 47 U. PITT. L. REV. 1037, 1040 (1986); Symposium, *Electronic Communication and Legal Change, Computer Network Abuse*, 6 HARV. J.L. & TECH. 307, 310-13 (1993) (concluding that the best means of maintaining information security is to establish a properly functioning computer security market). Predictably, a USA Today poll found that only 6% of Internet users wanted the federal government to administer it. James Kim, *Internet Users Favor Self-Regulation*, USA TODAY, Sept. 12, 1995 at B1.

19. TEDFORD, *supra* note 13, at 322.

printing presses.[20] As literacy spread and the fear of an informed public subsided, these prior restraints disappeared.[21] As a result, Blackstone defined free speech as that which existed in the absence of prior restraints.[22] Just as the technology of printing ingrained itself into the fabric of our society,[23] cryptography will play an indispensable roll in the digital age.

Cryptography, the craft of communicating in secret code,[24] is as old as written language.[25] The alphabet, for example, is simply a code we all understand.[26] The purpose of a secret code is to limit access to the contents of a message to a select group.[27] In other words, we use secret codes to keep secrets.

A. Symmetric Cryptography

Examined mathematically, there are two families of cryptographic systems.[28] Most familiar are symmetric cryptographic systems.[29] Both systems change one group of readable symbols into a second set of unreadable symbols.[30] Imagine a code which substitutes the original letters of a word with the letters which come two places earlier in the alphabet. In this manner, the message, "Free Speech" becomes "gsff qffdi."[31] The operation of substituting the letters is known as the "key" to the cipher.[32] In symmetric cryptography, the sender uses this key to encode his message and the receiver uses the same key to decode.[33] As long as the key remains a secret, it is impossible to read the message and the secret is safe.[34]

---

20. *Id.* at 6.

21. *Id.*

22. 4 William Blackstone, Commentaries 151-52.

23. Tedford, *supra* note 13, at 13-16.

24. Kahn, *supra* note 5, at xiii.

25. Hamilton Nickels, Codemaster: Secrets of Making and Breaking Codes 5 (1990).

26. Kahn, *supra* note 5, at 902 (arguing that the system of writing the ancient Greeks developed was a response to their encounter with a more complex code, Egyptian hieroglyphics).

27. Michael Kurland, The Spymasters's Handbook 5 (1988).

28. Berkovits, *supra* note 6, at 849; *see generally* Bruce Schneier, Applied Cryptography (1994) (surveying modern computer cryptography).

29. Berkovits, *supra* note 6, at 849.

30. *Id.* The set M is the actual message and is called the plaintext, while C, the encoded message, is known as ciphertext. *Id.* The entire operation is called a cipher. *Id.*

31. See Kurland, *supra* note 27, at 151 (giving a straightforward explanation of substitution ciphers).

32. Michael Kurland, The Spymaster's Handbook 151 (1988).

33. *Id.*

34. *Id.*

The practical weakness of symmetric ciphers is keeping the key a secret.[35] These systems require that both the sender and the receiver know the solution.[36] This means that at some point the parties must exchange unencoded information about the key[37] and thus the communication is always vulnerable to interception.[38]

Aside from interception, a more determined outsider can find the solution to symmetric ciphers by engaging in a series of experiments.[39] Attackers may try many different operations on the encoded message, hoping one attempt will reveal an intelligible message.[40] The time and effort necessary to mount this kind of attack is known as the "work factor" of a cipher, and rates its relative security.[41] One of the most sophisticated symmetric ciphers, the Data Encryption Standard ("DES"),[42] uses a 56-bit key.[43] To find the right key, an attacker is faced with seventy quadrillion combinations.[44] The work factor associated with DES prevents anyone armed with paper and pencil from ever finding a key.[45]

Using an ordinary desktop computer, however, an attacker could try all possible keys relatively quickly.[46] The rapid increase in computer

35. *Id.*

36. *See* KURLAND, *supra* note 27, at 851.

37. KURLAND, *supra* note 27, at 851.

38. KURLAND, *supra* note 27, at 851.

39. KAHN, *supra* note 5, at 399 (crediting Gilbert S. Vernam with creating virtually unbreakable code in 1917).

40. Berkovits, *supra* note 6, at 853. The search for keys through trial and error is known as an "exhaustive search" style of attack. *Id.* Other types of direct attacks include statistical attacks based on language usage, analytical attacks based on flaws in a cryptography system and traffic analysis which looks at the identity of the users. *Id.*

However, the difficulty of any given method of attack depends on what part of the message the cryptanalyist holds. *Id.* at 853. While an attacker in possession of ciphertext is generally harmless, one who holds some ciphertext and its companion plaintext is far more threatening. *Id.* The most dangerous attacker is one who can selectively examine specific segments of ciphertext and its corresponding plaintext. *Id.*

41. Berkovits, *supra* note 6, at 852. Since single-key systems rely on trial and error for security, they actually require shorter keys than asymmetric systems to achieve the same work factor. *Id.* Therefore, the work factor of a cipher is generally a multiple of the system's key length. Daniel Pearl, *Encryption-Software Plan Presented Using 'Keys' Held by Escrow Agents*, WALL ST. J., Aug. 18, 1995, at A3. Ominously, a French hacker recently cracked a 40-bit key, and even longer keys will become vulnerable soon. Berkovits, *supra* note 6, at 853.

42. Berkovits, *supra* note 6, at 854-55. An excellent directory of cryptography products is available on WWW Page: *Pointer to Cryptographic Software,* URL http://www.cs.hut.fi/crypto/software.html, created by Tatu Ylonen, viewed Nov. 18, 1995.

43. *Id.* DES uses eight nulls to check for errors or tampering in the transmitted message in addition to the 56-bit key. *Id.*

44. *Id.*

45. *Id.*

46. WALDO T. BOYD, COMPUTER CRYPTOLOGY 49 (1988).

processing speeds[47] led researchers in 1977 to predict that DES would be unable to protect information past the year 1990.[48]

B. Asymmetric Cryptography

In 1978, Ronald Rivest, Adi Shamir, and Leonard Adleman developed a revolutionary new style of cipher.[49] Named after its inventors, the RSA system employs a logarithmic function[50] to produce two keys.[51] By choosing a specific base number and an exponent, a sender can create a key that can be split between an encrypting function and a decrypting function.[52] Therefore, a party who wants to receive messages can publish part of the key[53] and keep the other part[54] a secret. With the public half,[55] a sender may encrypt messages, but only the person with the private key can decrypt them. This ability to receive messages without a loss to security is the genius of asymmetric cryptography.

In the summer of 1990, network users discovered the potential of asymmetric cryptography in a program called "Pretty Good Privacy."[56]

---

47. Vic Sussman, *The Devil of the Internet*, U.S. News & World Report, Apr. 17, 1995, at 12.

48. Berkovits, *supra* note 6, at 855.

49. Berkovits, *supra* note 6, at 856.

50. Berkovits, *supra* note 6, at 856. A logarithm is a mathematical expression which raises a base number by an exponent to produce a given, third number. Webster's II New Riverside University Dictionary 702 (1st ed. 1984).

51. Francis Litterio, WWW Page: *The Mathematical Guts of RSA*, URL: http: // draco.centerline.com:8080/~franl/pgp, created by Francis Litterio, viewed Nob. 18, 1995. Litterio simplifies the mathematics of RSA:

> 1. Find *P* and *Q*, two large (e.g., 1024-bit) prime numbers.
> 2. Choose *E* such that *E* and *(P-1)(Q-1)* are *relatively prime*, which means they have no prime factors in common. *E* does not have to be prime, but it must be odd. *(P-1)(Q-1)* can't be prime because it's an even number.
> 3. Compute *D* such that *(DE-1)* is evenly divisible by *(P-1)(Q-1)*. Mathematicians write this as *DE mod (P-1)(Q-1)*, and they call *D* the *multiplicative inverse* of *E*.
> 4. The encryption function is *encrypt(T) = (T^E) mod PQ*, where *T* is the plaintext (a positive integer) and '^' indicates exponentiation.
> 5. The decryption function is *decrypt(C) = (C^D) mod PQ*, where *C* is the ciphertext (a positive integer) and '^' indicates exponentiation.

Id. Litterio cautions that no one has proven that RSA does *not* have a mathematical weakness. *Id.*

52. Berkovits, *supra* note 6, at 855.

53. Litterio, *supra* note 51. The public part of the key is *(PQ,E)*. *Id.* Starting with only *(PQ,E)* an attacker cannot easily calculate *D*, *P* or *Q* and therefore a user can openly distribute the public half of the key. *Id.*

54. Litterio, *supra* note 51. The private part of the key is *D*. *Id.*

55. Berkovits, *supra* note 6, at 850.

56. William M. Bulkeley, *Cipher Probe: Popularity Overseas of Encryption Code has U.S. Worried*, Wall St. J. Europe, May 2, 1994, at A1. A few of the Internet sites offering PGP can be found on WWW Page: *M.I.T. Home Page*, URL: http://www.mit.ed/network/ pgp.html, viewed Nov 18, 1995; *see also*, WWW Page: *Mantis Home Page*, URL: http:// www.mantis.co.uk/ pgp/pgp.html, viewed Nov. 18, 1995.

Anonymously posted on the Internet,[57] the program produces its code using a RSA system.[58] The program, known as "PGP"[59] to users, was an immediate hit and it is still enthusiastically copied,[60] modified[61] and distributed all over the world.[62]

C. The Potential Advantages

The development of asymmetric encryption systems is not just a breakthrough in theoretical cryptography. Asymmetric systems allow businesses to exploit the economic potential of computer networks.[63] On the current networks, building a business on the Internet "is like trying to build a bank without walls."[64] Asymmetric cryptography provides tools for both security[65] and identification.[66] Businesses using asymmetric systems can deliver their products to consumers and protect their

57. Bulkeley, *supra* note 56.

58. Bulkeley, *supra* note 56.

59. *See* WWW page: *Frequently Asked Questions About Pretty Good Privacy,* URL: http://www.cis.tezcat.com/web/security, created by Andre Bacard, viewed Nov. 18, 1995.

60. *Id.* Zimmermann also distributes a cryptography product called the PGPfone which encodes ordinary telephone conversations. *Pretty Good Phone Privacy,* Newsweek, Aug. 28, 1995, at 10. PGPfone may be located on the internet using WWW Page: *Pointer to Cryptography Software,* URL: http://www.cs.hut.fi/crypto/software.html, created by Tatu Ylonen, viewed Nov. 18, 1995.

61. *Id.* PGP 1.0 uses RSA to protect DES keys during transmission, but employs DES to protect the body of the message. *Id.* PGP 2.0 and later versions use the Improved Data Encryption Algorithm ("IDEA") for the message. *Id.* An on-line warehouse of cryptography programs, such as IDEA, can be found at FTP: ftp.dsi.unimi.it; login: anonymous; password: e-mail address; directory: pub/security/crypt/code/, accessed Apr. 28, 1995. The most recent commercial version of PGP is 2.6.2 and the most recent freeware version is 2.7.1. Litterio, *supra* note 51. A draft of PGP 3.0 is also beginning to circulate. *See also* WWW Page: *Pointer, supra* note 42.

62. WWW Page: *Pointer, supra* note 42.

63. Mark L. Gordon & Diana J.P. McKenzie, *A Lawyer's Roadmap of the Information Superhighway,* 13 J. Marshall J. Computer & Info. L. 177, 182 (1995) (cataloging the various computer networks). Other networks include the National Information Infrastructure Testbed ("NIIT"), the National Research and Education Network ("NREN"), and private networks such as Prodigy, CompuServe, and America Online. *Id.* at 181-84. The networks also go by popular names such as the Net, the Web, the Cloud, the Matrix, the Metaverse, the Datasphere and, of course, the Information Superhighway. Philip Elmer-DeWitt, *Welcome to Cyberspace,* Time, Spring 1995, at 4. Today approximately forty million people around the world have access to the Internet. *Id.* at 9.

64. Nate Zelnick, *Keeping Business Safe on the Internet,* PC Magazine, Apr. 25, 1995, at 31 (outlining AT&T's Information Vending Encryption System ("IVES") chip).

65. David Post, *Encryption—It's Not Just for Spies Anymore,* Am. Law., Dec. 1994, at 106 (describing the Internet as "Dodge City"). Although 30,000 companies have Internet addresses, they are "simply showing their faces" because of the lack of security on the network. *Id.*

66. *See* Jill Gambon, *Signature Laws Near—California, Washington May Follow Utah Lead on Digital Signatures,* Information Week, May 8, 1995 at 24. The pioneering legislation in this area is the Utah Digital Signature Act, Utah Code §§ 46-3-101 et. seq. (1995).

property in ways simply not possible under conventional systems. In essence, asymmetric cryptography gives the networks the walls they desperately need.[67]

Cheap and convenient, asymmetric cryptography is not simply an economic device. It creates a new kind of speech-based privacy.[68] In Thailand, Guatemala and El Salvador, human rights activists are able to conduct work they otherwise would not risk through the use of cryptography.[69] During the Tiananmen Square uprising, Chinese dissidents used the cipher to communicate with the outside world.[70] The 1994 coup attempt in Russia generated a message, "[i]f dictatorship takes over Russia . . . PGP . . . will help democratic people if necessary. Thanks."[71] More ordinary users of PGP include an author who encrypts his work before sending it to his editor and an astronomer who encrypts his observations to prevent others from claim-jumping.[72] Around the world, cryptography is proving vital in protecting freedom.[73]

D. The Drawbacks

Unlimited privacy has a dark side as well.[74] For example, cryptography prevented the Los Angeles police from reading the diary of a child-pornography suspect.[75] It has also kept the police from reading the account books of fraud artists.[76] James Bidzos, who works for RSA Security, says he receives regular requests from police to help decipher

---

67. Charles L. Evans, Comment, *U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets*, 19 N.C. J. Int'l L. & Com. Reg. 469, 473 (1994).

68. Commercial software companies are also beginning to exploit the screening feature of cryptography. Jared Sandberg, *New Software Filters Sexual, Racist Fare Circulated on the Internet*, Wall St. J., May 15, 1995 at B12 (introducing a product that blocks offensive messages and searches for offensive sites).

69. Vic Sussman, *Lost in Kafka Territory*, U.S. News & World Rep. Apr. 3, 1995, at 32.

70. *Id.*

71. *Id.*

72. Bulkeley, *supra* note 56, at A1.

73. Bulkeley, *supra* note 56, at A1.

74. Symposium, *supra* note 18, at 310-13. Scholars identify six general areas of difficulty in network law enforcement. *Id.* First, spatial landmarks do not exist. *Id.* at 331. Second, criminal activity on a network is indistinguishable from lawful activity. *Id.* at 332. Third, it is difficult to positively identify users over a network link. *Id.* at 333. Fourth, traditional forms of proof will not work when the criminal's only contact with the scene of the crime was over a network. *Id.* at 334. Fifth, the "hearts and minds" of computer users are generally anti-government. *Id.* Sixth, current law does not sufficiently deter network abuse. *Id.* at 336.

75. Bulkeley, *supra* note 56, at A1.

76. Bulkeley, *supra* note 56, at A1.

encrypted information.[77] Law enforcement fears this is merely a shadow of what awaits them.[78]

Even before the age of asymmetric cryptography, the National Security Agency ("NSA")[79] saw a threat in private cryptography.[80] Goaded by the NSA, Congress categorized cryptography as an instrument of war and made it subject to the same kind of export restrictions as hand grenades and fighter planes.[81] Although the federal government has not yet restricted the domestic use of encryption,[82] it is promoting its own versions of digital security to wean the public away from private encryption.[83] In the government systems, the key to the system is held in the hands of an escrow agent who is charged with releasing it only in the event of an authorized request.[84]

However, escrow proposals are fundamentally flawed.[85] First, the proposal was developed amidst an aura of secrecy and mistrust.[86] Second, the resulting limit to surveillance does not warrant such elaborate government access to communications.[87] Third, ordinary citizens will not use an escrow system voluntarily.[88] Finally, without a better system of controls, an escrow system is prone to corruption.[89] In fact, public

77. Bulkeley, *supra* note 56, at A1.

78. Benjamin Wittes, *FBI, Justice Wary of Internet Crime; Info-Highwaymen Staying Far Ahead of Law Enforcement*, TEX. LAW., Oct. 24, 1994, at 8.

79. 50 U.S.C. §§ 401-32 (1988) (establishing the NSA).

80. JAMES BAMFORD, THE PUZZLE PALACE 351-55 (1982).

81. 22 C.F.R. § 121.1 (1993) (regulating hand-grenades and aircraft). The Arms Export Control Act includes, "cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information . . . ." Id. § 121.01; *see* John Perry Barlow, *Jackboots on the Infobahn*, WIRED 2.04, Apr. 1994 at 16.

82. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (signed into law on Oct. 25, 1994). Known as the 1994 Digital Telephony Act, this law places an affirmative duty on communications service-providers to cooperate with government interceptions. Id.

83. *See generally U.S. to Propose Federal Agency*, *supra* note 2, at B6. The most prominent of these escrow proposals is the Clipper Chip, a semiconductor which scrambles messages. FTP: *Vince Cate's Cryptorebel and Cypherpunk Home Page*, ftp://furmint.netcar.cs.emu.edu; login: anonymous; password: e-mail address; directory: security, accessed Nov. 18, 1995.

84. Philip Elmer-DeWitt, *Who Should Keep the Keys?*, TIME, Mar. 14, 1994, at 909-91.

85. Bruce Sterling, *So, People We Have a Fight on Our Hands*, WIRED 2.07, July 1994 (responding to pro-regulation arguments). On the other hand, organizations may need private escrow systems to prevent death or departure from exposing or permanently concealing information. *See* Don Clark, *Motorola Plans to Help Firms Protect Data*, WALL ST. J., May 15, at B12.

86. *Id.*

87. *Id.*

88. *Id.* at 2.

89. Hotz *supra* note 1, at B1. The government maintains 900 separate databanks consisting of billions of personal records and the General Accounting Office documented cases

reaction suggests that users will not accept any system managed by the state.[90]

The question of government regulation of cryptography is a threshold issue on the path to the Information Age.

III. AUTHOR'S ANALYSIS

The technology that is bringing the universe to our living rooms also threatens to eliminate privacy as we know it.[91] This Comment argues that direct state regulation of cryptography is an unconstitutional abridgement of free speech.[92] Part IIIA of this analysis addresses those arguments which classify cryptography as something other than speech.[93] Part IIIB addresses arguments that concede that cryptography is speech, but attempt to force it into an exception.[94] Part IV reveals the chilling effect of cryptography regulation on communications. Finally, Part V examines the market for cryptography and proposes that market mechanics provide a workable solution to the conflict over information security.[95]

A. CRYPTOGRAPHY AS NON-SPEECH

The line between electronic speech and traditional verbal speech is fading into oblivion.[96] As technology advances, the court's definition of speech tends toward unpredictable results.[97] Moreover, Congress has considerable power to regulate individual conduct[98] and even greater power to regulate goods and services.[99] Consequently, the issue of the status of encoded communication as "speech" is determinative.

---

where information from the FBI's National Criminal Information Center was sold to private parties; used to check up on political opponents and used to hunt down ex-girl friends. *Id.*

90. Zelnick, *supra* note 64, at 32.

91. Lennon, *supra* note 4, at 470 (arguing the regulation of cryptography violates Fourth Amendment).

92. *See* Stewart A. Baker, *Don't Worry Be Happy: Why Clipper is Good For You*, WIRED 2.06, June 1994, at 92 (outlining the general policy arguments in favor of government supplied encryption).

93. *See generally*, TRIBE & DORF, *supra* note 15, at 88.

94. TRIBE & DORF, *supra* note 15, at 89.

95. Symposium, *supra* note 18, at 342.

96. *See* Note, *infra* note 154, at 1083 (noting that all information will be reduced to a single digital medium); *see generally* WILLIAM S. DAVIS, THE INFORMATION AGE (William B. Gruener and Marion E. Howe eds., 1979).

97. LAWRENCE TRIBE, AMERICAN CONSTITUTIONAL LAW 827-30 (2d ed. 1988).

98. *See generally* United States v. O'Brien, 391 U.S. 367 (1968) (burning a draft card is conduct and subject to government control).

99. *See generally* Heart of Atlanta Motel v. United States, 379 U.S. 241 (1964) (using Commerce Clause power to regulate interstate commerce to support civil rights laws).

The distinction between speech and conduct is subject to scholarly criticism because of its unpredictability.[100] The Supreme Court defines flag-burning[101] as speech, while wearing campaign buttons is defined as conduct.[102] Regulators argue that cryptography is not speech at all.[103] The strength of this position is that encoded speech carries no message on its surface; since it does not look like speech, it is not speech.

In *Yniguez v. Arizonans for Official English*,[104] the U.S. Court of Appeals for the Ninth Circuit struck down an attempt to put an English-only amendment in a State constitution.[105] It held that a viewers' failure to understand a message simply means the communication is incomplete; it does not destroy that message's classification as speech.[106] To reach this conclusion, the *Yniguez* court first determined that speaking a foreign language is not a form of unprotected conduct any more than moving your mouth or typing on a keyboard.[107] Importantly, the *Yniguez* court stated foreign languages are speech by definition[108] and speech "in any language is still speech."[109] Using a foreign language involves the same fundamental choices as choosing words in a sentence.[110] The *Yniguez* court held that a state could not prohibit the personal choice of an entire vocabulary nor even a single word.[111]

Cryptography's similarity to a foreign language is unmistakable. Like a foreign language, unintelligible symbols can have a meaning, but only for those who understand the language. The sign language used by the deaf has little meaning for the unskilled, but carries the entire range of human emotion.[112] Using cryptography is like adopting a private language, "spoken" only by those who know the proper key. People send cards on birthdays, place calls to colleagues and send facsimiles to employees. Choosing to do each of these things in cryptographic language

100. TRIBE, *supra* note 97, at 827.

101. *See generally* Texas v. Johnson, 491 U.S. 397 (1989) (burning an American flag is speech and receives constitutional protection).

102. *See generally* Broadrick v. Oklahoma, 413 U.S. 601 (1973) (wearing political buttons is conduct in the government workplace).

103. Bulkeley, *supra* note 56, at A1.

104. 42 F.3d 1217, 1231 (9th Cir. 1994).

105. *Id.* at 1220.

106. *Id.* at 1231.

107. *Id.* at 1230.

108. *Yniguez*, 42 F.3d at 1230.

109. *Id.*

110. *Id.*

111. *Yniguez*, 42 F.3d at 1230. In *Cohen v. California*, 403 U.S. 15, 25 (1971), the Supreme Court endorsed a speaker's right to *choose* to say "fuck the draft," instead of some other expression of the same idea. The *Cohen* Court took the position that a government cannot "forbid the use of words without running the risk of suppressing ideas." *Cohen*, 403 U.S. at 26.

112. TRIBE, *supra* note 97, at 833.

does not make these messages less important. For the government to insist on a translation of each message simply because it does not understand the language is patently unreasonable. Simply because cryptography is a computer-based language, the courts should not strip it of constitutional protection.[113]

Another non-speech argument is that cryptography is a mechanical process rather than a form of speech. Theoretically, cryptography adds nothing to the message by putting readable material through an operation which makes it unreadable.[114] In a human sense, however, the transformation gives the message security and thus, influences its author.[115] The public availability of a message determines what a person reveals. The prudent person will presume that unencrypted messages are as public as a billboard and will restrain his expression accordingly. The creation of the message and the use of cryptography are inseparable.

A similar issue faced the Supreme Court in *Kovacs v. Cooper*.[116] The Court decided that the First Amendment protected the ideas transmitted by a loudspeaker, but that it did not protect the level of noise the loudspeaker produced.[117] In *Kovacs*, however, the Court focused on the intrusive nature of the loudspeaker and the protection of private homes.[118] Cryptography, on the other hand, does not pose any kind of invasion.

Moreover, cryptography requires the willing use of a key and thus implies an element of consent. Because asymmetric systems consist of a public key and a private key,[119] they create two filters for incoming messages.[120] The decision to view a message rests entirely with the receiver.[121]

In *Sable Communications, Inc. v. FCC*,[122] the Court addressed this consent issue when it struck down a prohibition on dial-a-porn services because the listener had to take affirmative steps to hear the message.[123] E-mail requires even greater affirmative steps to communi-

113. *Yniguez*, 42 F.3d at 1230.

114. Berkovits, *supra* note 6, at 849.

115. Lennon, *supra* note 4, at 483.

116. 336 U.S. 77, 86-87 (1949).

117. *Id.* at 85.

118. *Id.* at 87.

119. Berkovits, *supra* note 6, at 849.

120. Berkovits, *supra* note 6, at 851.

121. *See* Sable Communications of California, Inc. v. Federal Communications Comm'n, 492 U.S. 115, 128 (1989) (noting that placing a telephone call prevents the unintended surprises of pervasive mediums like radio).

122. 492 U.S. 115 (1989).

123. *Id.* at 121.

cate than in *Sable,* and cryptography goes a step beyond this.[124] Cryptography creates an unmistakable layer of consent. Therefore, unlike the situation in *Kovacs*, cryptography does not create a need for protective regulations to preserve the rights of others.

Undeniably, cryptography is a form of speech. A decision to use a code is one of the fundamental choices that underlie all expression.[125] Cryptography provides a form of security which directly alters language choices.[126] In addition, the affirmative conduct of the user creates a level of consent which separates cryptography from intrusive expression. Accordingly, definitions of speech that attempt to exclude cryptography fail.

B. The Exception Argument

1. *Established Speech Restrictions*

Beyond the issue of whether cryptography is speech, arguments could be advanced to limit these systems based on reasonable time, place and manner restrictions.[127] The unreadable nature of encoded messages means that these standards are a poor fit for cryptography.[128] The determinative question will be the legal status of the electronic networks where the systems operate.[129] While that issue lies beyond the scope of this Comment, it is possible to discuss cryptography in a public forum as well as a limited public forum.

i. Public Forum

The level of restriction a state may place on speech varies depending on nature of the forum.[130] Exchanges which take place on a public way, such as in a street, receive a great deal of constitutional protection.[131] In

124. *Id.* at 127-28; Jared Sandberg, *New Software Filters Sexual, Racist Fare on Internet*, Wall St. J., Sept. 20, at B12. SurfWatch Software offers a service which provides the addresses of offensive material. *Id.* Each month the company scans the Internet for words such as "pornography" and "pedophilia." *Id.*

125. *Yniguez*, 42 F.3d at 1231.

126. *See* Lennon, *supra* note 4, at 471.

127. *See generally* Schneider v. New Jersey, 308 U.S. 147 (1939) (banning all leaflets in an attempt to control litter was too burdensome on speech to be constitutional); Konigsberg v. State Bar of California, 366 U.S. 36, 49-51 (1961), *reh'g denied*, 368 U.S. 869 (1961). Although the *Konigsberg* Court held that the freedom of speech is not "an unlimited license to talk," Justice Black took the position that the words of the First Amendment indicate an underlying absolute freedom. *Id.* at 59-60 (Black, J., dissenting).

128. Tribe & Dorf, *supra* note 15, at 88.

129. Edward J. Naughton, *Is Cyberspace a Public Forum? Computer Bulletin Boards, Free Speech, and State Action*, 81 Geo. L. J. 409, 414 (1992).

130. Tribe, *supra* note 97, at 791-92.

131. *See generally* Hague v. C.I.O, 307 U.S. 496 (1939) (holding that the public's use of streets for debate is an ancient form of liberty).

a computer network, however, the limits of physical space evaporate.[132] Events which ordinarily occurred on the street take place between machines scattered all over the globe.[133]

Presumably, with the Internet doubling in size every year,[134] it will soon earn the title of public forum.[135] Any restrictions on speech in a public forum must serve a compelling public interest and be narrowly tailored to serve that interest.[136] The argument is that wide availability of cryptographic technology creates a compelling threat to the safety of American citizens because it erodes the ability of government to gather evidence.[137] However, cryptography functions like a ski-mask, only obscuring a robber's identity; it is not inherently dangerous.[138] Further, misuse of cryptography does not eliminate the ability of police to gather evidence; it only prevents them from understanding it.[139]

Furthermore, no regulation could ever be sufficiently tailored to the goal of crime prevention[140] to survive constitutional scrutiny.[141] A cryptography regulation would attach equally to any sort of speech the user encoded, from pornography to political debate. In a public forum, the government's limited interest cannot support cryptography regulation.

ii. Limited Public Forum

In a limited public forum, the government creates or authorizes the public's use and therefore, it has a greater power to regulate speech.[142] The regulation must be reasonable in light of the purpose of the forum; it must be viewpoint neutral and it must leave open alternate channels of expression.[143] Advancing the same safety interests, the fit between reg-

132. Teri A. Cutrera, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 UMKC L. Rev. 139, 142 (1991).

133. Naughton, *supra* note 129, at 413.

134. Survey, *The Accidental Superhighway*, ECONOMIST, July 1, 1995, at 3.

135. *See* Eric C. Jensen, *An Electronic Soapbox: Computer Bulletin Boards and the First Amendment*, 39 FED. COMM. L. J. 217 (1987).

136. In *Brandenburg v. Ohio*, the Supreme Court reversed a conviction under a criminal anarchy law where the speaker advocated racial violence in a television interview. 395 U.S. 444, 446 (1969) (per curiam). The *Brandenburg* Court stated that for the government to criminalize speech, the speaker would have to intentionally incite lawless action. *Id.* at 447.

137. Bulkeley, *supra* note 56, at A1.

138. Bacard, WWW *Page*, *supra* note 59.

139. Lennon, *supra* note 4, at 473.

140. Nina Schuyler, *Bugs in the System, The FBI Wants to Monitor Traffic on the Information Superhighway*, CAL. LAW., July 1994. at 149 (noting that the government seems to want access to all information).

141. LAWRENCE TRIBE, AMERICAN CONSTITUTIONAL LAW 830 (2d ed. 1988).

142. *Id.* at 831.

143. *Id.*

ulating cryptography and crime prevention suggests the same police power argument for regulation in a limited public forum.[144]

In *International Society for Krishna Consciousness v. Lee*,[145] the Supreme Court established a yardstick for reasonableness in a limited public forum.[146] It upheld a regulation prohibiting the solicitation of donations in an airport terminal because the regulation promoted safe traffic flow in an airline terminal.[147] While not the most narrowly tailored approach, the *Krishna* court reasoned that in this non-traditional forum, the regulation only needed to reflect the purpose of the forum and exhibit viewpoint neutrality.[148] The focus of the court was the purpose of the terminal and in that light, the regulation was reasonable.[149]

The use of cryptography on the Internet is distinguishable from the airport solicitation in *Krishna*. The purpose of the Internet and other computer networks is to carry information.[150] While restricting panhandlers may be reasonably related to getting commuters safely through an airport, regulating the only source of protection on the network will not speed the flow of information. It may create such weaknesses that users will avoid the networks when transferring data.[151] Restrictions on the amount and type of private communications an individual enjoys is antithetical to free and public exchange.[152]

As to the alternate channels, the approach of complete communications integration means that improperly conceived, drafted or implemented regulations will result in utter exposure.[153] This underlines the reality that in either forum, the presence of government regulation places all our communications at risk.[154]

IV. PRIOR RESTRAINT AND CHILLING EFFECT

Independent of the forum,[155] the least tolerable restrictions on speech occur when government attempts to prevent the expression of

144. *Id.* at 982.
145. 112 S. Ct. 2701 (1992).
146. *Id.* at 2703.
147. *Id.* at 2701.
148. *Id.* at 2704.
149. *Id.*
150. Gordon & McKenzie, *supra* note 63, at 179.
151. Bulkeley, *supra* note 56, at A1.
152. *Id.*
153. *Id.*
154. *See* Note, *The Message in the Medium: The First Amendment on the Information Superhighway*, 107 HARV. L. REV. 1062, 1083 (1994) (arguing the case for uniform treatment of all telecommunications).
155. *See generally* Schenck v. United States, 249 U.S. 47 (1919). In *Schenck*, a unanimous Supreme Court held that pamphlets urging recruits to oppose the draft rose to the

particular ideas.[156] Prior restraints strike at the heart of our First Amendment freedoms.[157] Because encrypted communications are unquestionably speech, cryptography regulations are a form of prior restraint.

To prove the necessity of a prior restraint, the state carries a heavy burden.[158] An informed public is the primary shield against misgovernment,[159] and the government must show that the threat to the nation's well-being posed by the publication of the idea outweighs this safeguard.[160] The indirect connection between a stream of unreadable ciphertext and a vague threat of a national crime wave will not support a prior restraint.[161] The government could never carry this burden.

In the only case ever directly upholding a prior restraint, *United States v. Progressive*,[162] the District Court for the Western District of Wisconsin enjoined the publication of a magazine article describing how to build an atomic bomb.[163] The *Progressive* court allowed the first prior restraint in this nation's history after it balanced the risk to the human race against the magazine's First Amendment rights.[164] The oddity of the *Progressive* case suggests that the threat posed by the information must be cataclysmic.[165] The government interest in cryptography, however, is considerably less than the survival of our species.

---

level of a "clear and present" danger because of the "character of the act [and the] circumstances in which it [was] done." *Id.* at 52.

156. Grosjean v. American Press Co., 297 U.S. 233, 250 (1936). In *Grosjean*, Louisiana enacted a tax on advertising receipts of newspapers. *Id.* at 234. Finding this tax to be unconstitutional, the *Grosjean* Court took the First Amendment to be a clear rejection of England's historical system of prior restraints. *Id.* at 249.

157. Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976). In *Nebraska Press*, the Supreme Court struck down an injunction on newspaper publication of a murderer's confession.

Id. at 562. Although the publication might infringe upon the ability to receive a fair trial, the *Nebraska Press* court held that the state would have to show definite harm to merit an injunction. *Id.* at 563.

158. Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546, 558 (1975). Without actually seeing the production, the Chattanooga, Tennessee city council banned the production of the musical *Hair* because it contained nudity. *Id.* at 548-49. Justice Douglas took the position in his dissent that the Constitution prohibits all censorship, no matter how brief. *Id.* at 563 (Douglas J., dissenting).

159. *Grosjean*, 297 U.S. at 245-50.

160. Near v. Minnesota, 283 U.S. 697, 716 (1931) (stating that publishing the dates and times of military operations would justify a prior restraint).

161. New York Times v. United States, 403 U.S. 713, 715 (1971) (denying an injunction where publication would embarrass the executive branch).

162. 467 F. Supp. 990 (W.D. Wis. 1979)

163. *Id.* at 994.

164. *Id.* at 996.

165. *Id.* at 995 (noting that the consequence of error with regard to atomic bombs involves "life itself").

While direct regulation is generally unconstitutional, government attempts to impose self-censorship are also unconstitutional.[166] In *New York Times v. Sullivan*,[167] the Supreme Court addressed the issue of self-censorship "chilling" newspaper reporting.[168] Any errors, even unintentional ones, gave a plaintiff grounds to sue and win a libel action under the existing libel standard.[169] Citing a "profound national commitment"[170] to open, uninhibited public debate, the *Sullivan* Court found that a free press could not operate under such a continual threat of civil action.[171]

Restricting cryptography will favor eavesdroppers, snoops and thieves to the point where it will unconstitutionally censor speech. With machine-driven searches, anyone can continuously scour millions of bits of information.[172] In *Sullivan*, the guarantees of the First Amendment mandated that the Court construe the libel laws to prevent indirect censorship.[173] Surveillance technology is eroding these same guarantees.[174] If cryptography is to restore the constitutional balance, it must be free of the dead hand of government regulation.

V. A SOLUTION

The same technology that makes it possible to scan an encyclopedia in seconds vastly expands the government's power to monitor our speech[175] and threaten our constitutional freedoms.[176] Law enforcement agencies fear cryptography will counter its current advantage or worse, tip the balance in favor of lawlessness.[177] On the other hand, sophisticated private cryptography is an inescapable necessity if computer networks are ever to rise to their potential. The solution lies in letting these divergent interests compete in the marketplace.

---

166. TRIBE, *supra* note 97, at 946.

167. 367 U.S. 254 (1964)

168. *Id.*

169. *Id.*

170. *Id.* at 256.

171. *Id.*

172. Hotz, *supra* note 1, at B1.

173. *New York Times*, 367 U.S. at 258.

174. Thomas J. Emerson, THE FIRST AMENDMENT IN THE YEAR 2000, THE FUTURE OF OUR LIBERTIES 70-71 (Stephen C. Halpren ed., 1982).

175. Wittes, *supra* note 78, at 8. In the days of paper mail, "[individuals] were like little mammals scurrying . . . between the legs of the giant dinosaurs. But now, the government dinosaur has acquired the nervous system of a ferret." *Id.*

176. Lennon, *supra* note 4, at 467, 467 n.2.

177. Hotz, *supra* note 1, at B1.

A. The Marketplace

A marketplace for any commodity is made up of all the exchanges between suppliers and consumers.[178] This interaction serves three vital functions in a society.[179] First, it mediates the conflict between those who have a commodity and those who want it.[180] Second, the marketplace allocates limited resources in an efficient manner.[181] Finally, markets provide people with vital feedback about the decisions they make.[182] When the marketplace is composed of a large number of suppliers; a large number of consumers; and trades in a fungible good, it is competitive and serves its social functions efficiently.[183] Importantly, competitive markets develop wherever there is a demand—with, without, or in spite of government initiatives.

B. The Market for Cryptography

Cryptography systems can take the form of hardware, like semiconductor chips imbedded in appliances, or software which runs as a program.[184] Cryptography software has several advantages over hardware systems. Software is flexible enough to work with a variety of machines and can respond to an assortment of user needs.[185] It can be easily inspected to make sure it does what it claims.[186] Most importantly, since software is cheap to produce and distribute, sellers can disseminate innovations quickly.[187] These advantages mean that software cryptography systems will eclipse hardware systems for the foreseeable future.[188]

Similar to the software market, the cryptography market has all the elements to be a purely competitive market. Every single one of the millions of personal computers around the world is a potential factory.[189] Every computer, telephone and facsimile machine is a potential consumer.[190] The rapidly expanding reach of computer networks means the market for cryptography is vast.[191] With manufacturers able to jump in

178. Robert P. Thomas, Economics: Principals and Applications 86-87 (1990).
179. *Id.* at 104.
180. *Id.*
181. *Id.*
182. *Id.*
183. Thomas, *supra* note 178, at 101.
184. *Don't Tell it to the Spartans*, *supra* note 7, at 81. Hardware and software combined, the market for cryptography products will reach $3 billion by 1999. Clark, *supra* note 85, at B12.
185. *Don't Tell it to the Spartans*, *supra* note 7, at 81.
186. *Id.*
187. *Id.*
188. *Id.*
189. Boyd, *supra* note 46, at 48.
190. *Id.*
191. Gordon & McKenzie, *supra* note 63, at 180.

and out of the market effortlessly, no one supplier nor single buyer can substantially influence the market price.[192] There are few distribution problems on computer networks.[193] Further, the implementation of any one cryptographic program is indistinguishable from any other and therefore, consumers can change systems without penalty.[194] Consequently, the market for software-based cryptography is almost ideally competitive.

The appeal of the marketplace solution is its effect on the underlying commodity, information security. First, open markets allow those who desire security to obtain it in some form.[195] A large number of producers will produce a variety of products and distribute them to wide assortment of consumers facing different problems all over the world.[196] Second, the cryptography marketplace efficiently allocates the time and talent which creates it.[197] Those consumers who desire the most protection will hire those mathematicians and programmers who show the most ability.[198] Government, which invariably possess more resources than private individuals, can also pursue its goals.[199] Further, the ease of market entry allows any "weekend programmer" a chance to innovate and explore for customers in the market.

Finally, the cryptography market provides manufacturers and consumers with information about their decisions. Users send a message through their purchases to producers about the level of protection they desire.[200] Manufacturers respond by developing new cryptography products or by eliminating existing ones.[201] An uncontrolled cryptography market allows citizens to feel safe, nurtures innovation and allows for rapid responses to changing threats.

---

192. *See* THOMAS, *supra* note 178, at 87-88 (noting competitive markets cannot have significant barriers to entry or exit).

193. *See id.* at 148.

194. *See id.* at 88 (noting the ability to switch between goods without significant penalty is essential in a competitive market).

195. THOMAS, *supra* note 178, at 88.

196. *See id.* at 149 (emphasizing the importance of technology to suppliers).

197. *Id.* at 88-89.

198. See BOYD, *supra* note 46, at 52.

199. *Id.* Rather than compete against its citizens, the FBI is currently pursuing an Orwellian scheme to build government access into the nation's phone network. John Markoff, *FBI Wants Advanced Systems to Vastly Increase Wire Tapping*, NEW YORK TIMES, Nov. 2, 1995 at A1.

200. THOMAS, *supra* note 178, at 101.

201. *Id.* at 10.

C. Flaws in the Marketplace Solution

The marketplace alternative has two potential problems.[202] First, the currently ideal market may not always maintain its integrity. Sudden changes in availability of the related hardware, compatibility or in the nature of the expected threats might leave some consumers dangerously exposed.[203] Unexpected technological breakthroughs or roadblocks might drive the less resourceful producers out of the market and limit the number of options open to the public.[204] However, shifts in the market are, at least in part, created by the market[205] and the cryptography industry should be able to absorb temporary imbalances.

The second problem is whether cryptographic security has evolved from a desire into a *need*.[206] The word need suggests that for this resource, there is an absolute acceptable minimum.[207] If an individual should fall below this level, society is willing to make a sacrifice in order to restore that level.[208] If programs which automate cryptographic attacks, like SATAN,[209] have brought us to a place where any unencrypted message is essentially open to the public,[210] the question is whether we are willing to make a sacrifice in order to establish a minimum level of cryptographic protection. The threat forces us to insist that our banks, our hospitals, and our schools protect themselves in order to protect us. If its absence directly restricts our ability to express ourselves, cryptography becomes a necessity and a right.

---

202. *Id.* at 101.

203. *Id.* at 181.

204. Thomas, *supra* note 178, at 312-13.

205. *Id.* at 8-12 (stating markets are the result of scarcity).

206. *Id.* at 92-94.

207. *Id.* at 92

208. *Id.* at 93-94.

209. Sussman, *supra* note 47, at 12. Weaknesses in network software appear with some regularity. *See e.g., Netscape Reassures Users Internet Software is Safe*, Wall St. J., Sept. 20, 1995, at B10. SATAN automates the techniques hackers use to identify and exploit weaknesses in networks. Sussman, *supra* note 47, at 12. Other programs such as LocalPeek, NetMinder and Traffic Watch allow network managers to eavesdrop at will. Bacard, WWW Page, *supra* note 59. Wpcrack, designed to break WordPerfect's encryption system, is available at FTP: ftp.dsi.unimi.it; login: anonymous; password: e-mail address; directory: /pub/security/crypt/code, accessed Apr. 28, 1995.

To counter the flaws in its system, Netscape began a policy of rewarding those users who find bugs. Joan E. Rigdon, *Netscape is Putting a Price on the Head of Any Big Bug Found in Web Browser,* Wall St. J., Oct. 11, 1995, at B8. In addition, Netscape plans to make its software compatible with the United States government multilevel information security system, code-named Fortezza. *U.S. Cryptography Adopted,* Wall St. J., Oct. 11, 1995, at B8; *see also, Mykotronx Announces Award of High Grade Crypto Processor Program,* Bus. Wire, Oct. 2, 1995, at 109.

210. Boyd, *supra* note 46, at 49.

V. CONCLUSION

Surveillance technology threatens to eliminate private communication in the near future and to unconstitutionally abridge free speech. Cryptography promises to provide an inexpensive and adaptable shield against this intrusion. Moreover, encryption technology gives business the equipment necessary to develop on the networks. On the other hand, government fears that terrorists and criminals will exploit this technology, and so seeks to regulate its use. The conflict over cryptography requires us to balance our fears against our beliefs.

The solution lies in putting control of cryptography in the marketplace. The nature of the market assures that it can produce a variety of affordable and effective cryptographic systems. Left to itself, this industry will foster originality and provide a flexible response to new threats. Structural inequalities in the cryptography market, which might leave some people unprotected, have yet to appear. In the digital age, technology infringes on our ability to communicate and abridges our First Amendment rights. Cryptography can restore that fundamental privacy and it is an indivisible part of our freedom.

PHILLIP E. REIMAN