William & Mary Bill of Rights Journal

Volume 4 (1995-1996)
Issue 3

Article 11

May 1996

Freedom to Speak Unintelligibly: The First Amendment Implications of Government-Controlled Encryption

Jill M. Ryan

NOTES

FREEDOM TO SPEAK UNINTELLIGIBLY: THE FIRST AMENDMENT IMPLICATIONS OF GOVERNMENT-CONTROLLED ENCRYPTION

The emergence of the computer has revolutionized communications, allowing quick dissemination of information to large numbers of people. Information transmitted electronically is often safeguarded through a widely available method known as encryption, which renders the information unintelligible to anyone without the ability to decrypt the message. Law enforcement agencies argue that unregulated encryption hinders their ability to prevent crime by providing criminals with a method of communication that cannot be accessed by police departments and government agencies. Proponents of encryption argue that privacy, security, and constitutional concerns outweigh law enforcement's fears, guaranteeing the ability to communicate confidentially.

In 1994, the government adopted a new encryption standard that arguably alleviated the risks underlying confidential communications. This Note will argue that although voluntary, this action was a failed attempt at controlling encryption, and that as a result, the federal government will propose a mandatory encryption scheme. Under traditional First Amendment jurisprudence, such a scheme resembles a content-neutral time, place, and manner restriction, and courts will have to balance the competing interests involved. This Note analyzes the First Amendment implications of a mandatory encryption scheme, including possible chilling effects on speech.

* * *

"In some times and places the even more capricious new media will open wider the floodgates for discourse, but in other times and places, in fear of that flood, attempts will be made to shut the gates."[1]

INTRODUCTION

As Pool predicted over a decade ago, we are now entering a revolution in communications with the emergence of what has become known as the "information superhighway." This superhighway is becoming the means by which information—be it voice, data, image, or video—is transmitted, and consists of all broadcast media, cable television, telephones, and other com-

[1] ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM 251 (1983).

munications systems.[2] This highway runs through "cyberspace,"[3] which is already global and is expected to permeate all facets of life.[4]

The floodgates of discourse thus have been flung open, as more kinds of information can be exchanged with more people more quickly and efficiently than the Framers of the Constitution could have ever dreamed. Computers, once marveled simply for their superiority over both the typewriter and the calculator, have become a direct line to the rest of the world. Computer networks and electronic information services provide many functions: users communicate with each other by electronic mail (e-mail), they access electronic bulletin boards on particular topics, and large networks provide information in all kinds of databases, some of which allow users to download data onto their own computer.[5] "The vast array of networks emerging have led some commentators to muse that it will be possible for people to live and work in a world of information [cyberspace] rather than in what is now thought of as the 'real' world."[6]

This medium is growing and expanding so fast that few can keep up with it—especially the law. Providing easier access to and transmission of information not only can facilitate garden-variety crimes,[7] but also gives

---

[2] Andrew Grosso, *The National Information Infrastructure*, 41 FED. B. NEWS & J. 481, 481 (1994).

[3] John Perry Barlow "first borrowed the term 'cyberspace' from science fiction and applied it to the disembodied universe of computer networks and bulletin boards like the Internet." Charles McCoy, *Visionary or Space Cadet*, WALL ST. J., Nov. 14, 1994, at R20. Nevertheless, "cyberspace" has come to encompass more than simply a chain of computer networks. For example, Barlow describes the Internet as "a self-perpetuating organism . . . dividing, multiplying, and expanding to fill the vast void of cyberspace." *Id.* *See* Curtis E.A. Karnow, *The Encrypted Self: Fleshing Out the Rights of Electronic Personalities*, 13 J. MARSHALL J. COMPUTER & INFO. L. 1 (1994); *see also* Grosso, *supra* note 2, at 481 (referring to cyberspace as a "world of information").

[4] "[I]t will connect every home, office, news medium, library, data bank, business, government agency, and computer to every other such entity, and to every person who uses a communications device, such as a telephone, television, or personal computer." Grosso, *supra* note 2, at 481.

[5] Note, *The Message in the Medium: The First Amendment on the Information Superhighway*, 107 HARV. L. REV. 1062, 1067 (1994).

[6] Grosso, *supra* note 2, at 481.

[7] Some examples are criminal solicitation and conspiracy, distribution of pornography, fraud, and terrorism. *See* Scott Bowles, *Police Search of AOL Files Divides the On-Line World*, WASH. POST, Jan. 26, 1996, at A1, A24 (discussing police's search of America Online's computer records for information concerning a New Jersey murder); Michael Meyer, *The Bad Dream Comes True in Cyberspace*, NEWSWEEK, Jan. 8, 1996, at 65 (describing Compuserve's decision to cut off access to pornographic material on the Internet because it violated Germany's pornography laws).

rise to new types of crimes, many of which are aimed at the transmitted information.[8] In short, new technology can make life easier for everyone, not just the law-abiding.

To safeguard networked information, researchers have developed encryption, a process which allows a sender to "code" an electronic message either before or as it is being sent.[9] The receiver must then know how to "decode" the message in order to read it.[10] As a result, if an unauthorized person intercepts an encrypted transmission, the content of the transmission is unintelligible to them, and the information remains confidential. Encryption, however, has the added feature of being nondiscriminatory—it "shields the law abiding and the lawless equally."[11] Federal, state, and local law enforcement agencies fear that encryption will allow criminals and terrorists to hide their illegal activities, a fear driven by the fact that encryption products now are widely available that are so strong as to be "uncrackable" by government cryptography experts.[12]

Not surprisingly, the government is trying to control the use and availability of the stronger encryption products, though it has stopped short of either banning encryption altogether or restricting encryption to only a few acceptable methods. Nevertheless, in order to adequately address the government's fears, the government must enact a mandatory encryption scheme. Such a measure raises a host of social, political, and constitutional concerns for the users of encryption, and for society in general.

Part I of this Note will examine electronic communications, including the use of computer networks and the threats to networked information. This Note will then explain the functions and use of encryption as one method for safeguarding this information, along with the corresponding policy con-

---

[8] *See* Scott Charney, *Computer Crime*, 41 FED. B. NEWS & J. 489, 489 (1994) (listing three ways computers are used for crimes: another computer as the target of the crime, the computer as a tool of the crime, or the computer that holds evidence of the crime). *See generally* DAVID ICOVE ET AL., COMPUTER CRIME: A CRIMEFIGHTER'S HANDBOOK (1995) (discussing types of computer crimes and the means of handling them).

[9] *See* discussion *infra* part I.C.

[10] *See* Herb Brody, *Of Bytes and Rights*, TECH. REV., Nov./Dec. 1992, at 22, 26 (explaining that encryption "ensures that only the person for whom the message is intended will read it").

[11] Steven Levy, *Battle of the Clipper Chip*, N.Y. TIMES, June 12, 1994, § 6 (Magazine), at 44, 46.

[12] RSA, the best known public-key cryptosystem, allegedly can be broken, but it would take the world's fastest computers hundreds or thousands of years. Jeff Prosise, *How to Keep It a Secret*, PC MAG., July 1994, at 315, 321. Another allegedly unbreakable program is Pretty Good Privacy (PGP), an encryption program developed by Philip Zimmerman, who gave it away for free as a means of ensuring the availability of good cryptography, regardless of the government's actions. Levy, *supra* note 11, at 60; *see also infra* notes 53-55 and accompanying text.

siderations of the government in regulating encryption. Part II will examine the government's largely unsuccessful attempts to control encryption, and the many social and political arguments that disfavor future government attempts at such control. This Note then assumes that some type of a mandatory encryption scheme eventually will result and examines the First Amendment free speech implications of mandatory encryption. Part III begins by surveying the array of constitutional arguments that have been levied against mandatory encryption. This Note will begin the First Amendment examination by identifying the analytical difficulties posed by electronic communications as a whole. Next, mandatory encryption will be analyzed under traditional First Amendment jurisprudence as both a content-based and content-neutral regulation. Finally, this Note will examine the potential chilling effect that mandatory encryption would have on the exercise of free speech.

I. ELECTRONIC COMMUNICATIONS AND ENCRYPTION AS THEIR PROTECTOR

A. *Electronic Communications and Networked Information*

Electronic communications offer a number of advantages over traditional paper-based communications: speed, low cost, great storage capacity, rapid and convenient access, content-based access, and better reproducibility.[13] These advantages are possible because the information is digitized;[14] in a sense, the information is broken up into bits that are transmitted and reassembled at the receiver's end. As a result, the time required to access, transmit, and publish information has been reduced significantly, and the amount of information that can be stored is almost unlimited.[15] All of these factors combined result in the ability to transmit instantly vast amounts of information around the world to as few or as many people as desired.

---

[13] Martin E. Hellman, *Implications of Encryption Policy on the National Information Infrastructure*, 11 COMPUTER L. 28, 28 (1994). For a more detailed explanation on transmission, storage, organization, and processing of information in the electronic setting, see M. Ethan Katsh, *The First Amendment and Technological Change: The New Media Have a Message*, 57 GEO. WASH. L. REV. 1459, 1473-79 (1989).

[14] Katsh explains that:

> [d]igitalization is a process in which some record of reality is broken up into many parts and each part is assigned a numerical value. Pictures, for example, are not treated as whole images but as thousands or millions of dots, each of which can be identified by number. Words or pictures are communicated electronically by placing them into a machine that performs this numbering process, converts the numbers to electronic signals, sends the signals to some other place, and then reverses the process and transforms the signal back into the original form.

Katsh, *supra* note 13, at 1476.

[15] *Id.* at 1473, 1475.

With the ability to both process and communicate information, computers operate at maximum efficiency when linked to other computers.[16]

> Under such circumstances, information can have rapid global impact simply by remaining in a computer that is linked to other computers. Information can reach larger audiences more rapidly and can be responded to and passed on to others more quickly. This process of information growth is accelerated as bottlenecks retarding the growth of knowledge are removed and as methods of research and publication change.[17]

A network is simply two or more computers linked together, and two or more networks linked together often are referred to as an internetwork.[18] The largest, and certainly the most well-known system of interconnected computer networks is the Internet,[19] which "[b]y mid-1994 . . . had reached 100 countries and all seven continents, with about 600,000 host machines connected, and a user population in the multi-millions. The Internet is now doubling in size every 9 to 10 months."[20]

As the size of networks and number of users has expanded, so has the use of computer networks in daily life. One need only look to the growth of electronic mail to realize the personal and inter-office importance of this means of communication. Even more staggering is the amount of business transacted over networks, particularly within the financial community. The Office of Technology Assessment (OTA) reports that:

> the average number of electronic point-of-sale transactions in the United States went from 38 per day in 1985 to 1.2 million per day in 1993. An average of $800 billion is transferred among partners in international currency markets ev-

---

[16] *Id.* at 1473.

[17] *Id.*

[18] *See* ICOVE ET AL., *supra* note 8, at 130. Networks commonly are referred to as one of several different types: local area networks (LANs), wide area networks (WANs), and internetworks. *Id.* For purposes of this Note, the term "networks" is meant to be all-encompassing, because the First Amendment analysis should not change regardless of the type of network involved.

[19] The Internet grew out of the first computer network, the Department of Defense's Advanced Research Projects Agency Network (ARPANET). Grosso, *supra* note 2, at 481. "ARPANET grew out of an earlier plan for a network intended to function in the event of a nuclear war. For that reason, it was designed with no central command which might be vulnerable to an outside attack." *Id.* For a description of how information gets routed through this maze of computers, see *id.* at 481-82.

[20] *See* ICOVE ET AL., *supra* note 8, at 131.

> ery day; about $1 trillion is transferred daily among U.S. banks; and an average of $2 trillion worth of securities are traded daily in New York markets. Nearly all of these financial transactions pass over information networks.[21]

Add to that the use of electronic communications in government, national defense, and in our health care systems, and the fact is clear that electronic communications play not only a major, but a crucial role in our lives.

B. *Threats to Networked Information*

While digitalization makes communication faster, easier, and more efficient, it also makes electronic communications less secure than traditional forms of communication:

> Electronic communication is inherently more vulnerable to interception than conventional forms of communication. Phone calls can be tapped one at a time, but the tapper must listen to the whole conversation. Paper mail can be intercepted, but it is laborious to search large quantities. By contrast, every e-mail message or bulletin board posting is stored on a central computer so that it can be forwarded to its recipient or broadcast to all network subscribers. Once stored, electronic messages can be searched for certain words, phrases, or names. Surveillance takes on an ominous new dimension.[22]

Furthermore, this vulnerability increases as the number of computers networked together increases. Each computer through which a user communicates "may have hundreds of other users and may be connected to numerous other networks. At any point, there is a possibility that an eavesdropper may tap into [the user's] message."[23]

Although many factors threaten computer networks and the information they contain,[24] one of the most serious is the problem of "hackers," persons whose goal is to break into computer systems.[25] The most common targets

---

[21] OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 1-2 (1994) [hereinafter OTA, INFORMATION SECURITY] (footnotes omitted).

[22] Brody, *supra* note 10, at 26.

[23] ICOVE ET AL., *supra* note 8, at 132.

[24] Some of these factors include human errors, design faults, insiders, natural disasters and environmental damage, and viruses and other malicious software, to name just a few. OTA, INFORMATION SECURITY, *supra* note 21, at 25-26.

[25] Hackers seek to obtain unauthorized access to computer systems for three reasons:

include military and intelligence computers targeted by espionage agents, businesses targeted by competitors, banks and financial organizations, terrorist attacks, companies targeted by employees or ex-employees, and hackers or "crackers" targeting systems solely as an intellectual challenge.[26] Although the hackers' targets *could* be private communications, the sheer volume of business transactions and government communications conducted over computer networks makes those entities more attractive and especially vulnerable targets. Estimates reveal that eighty-five to ninety-seven percent of computer intrusions go undetected.[27] As a glimpse of the future, the Pentagon reportedly is developing strategies for cyberspace warfare, also known as infowar, designed to both defend and wreck computer systems during conflicts.[28]

Thus, the consequences of easy access to information is more than just a pesky hacker reading someone's private e-mail. The information contained in networks is in danger, and unauthorized access can create an ominous ripple effect throughout society.

C. *Encryption As a Method for Safeguarding Networked Information*

In attempting to minimize the threats to networked information without surrendering the advantages of such communications, several methods of safeguarding networked information have been developed.[29] "There are many ways to secure sensitive data files from unauthorized access, but few are as effective—or as convenient—as encrypting them."[30] Encryption does not prevent someone from intercepting the data being sent, but it prevents that person from being able to use the information.[31] Encryption relies on

---

(1) for profit or some other benefit, (2) for revenge, or (3) as a game or challenge. 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, 470 (1994).

[26] *See* ICOVE ET AL., *supra* note 8, at 5-15.

[27] *Id.* at 3. The Department of Defense recently sponsored a test, wherein "[a]ttempts were made to attack a total of 8932 systems . . . . 7860 of those systems were successfully penetrated. The management of only 390 of those 7860 systems detected the attacks, and only 19 of the managers reported the attacks." *Id.*

[28] Neil Munro, *The Pentagon's New Nightmare: An Electronic Pearl Harbor*, WASH. POST, July 16, 1995, at C3. "Infowar" is defined as "the effort to seize control of electronic information systems during a conflict." *Id.*

[29] Tools that are currently available include challenge-response systems, secure tokens, firewalls, virus checkers, auditing and intrusion detection, encryption, digital signatures, biometric devices, and separations of duties. OTA, INFORMATION SECURITY, *supra* note 21, at 32-40. For a description of these methods and a detailed study of safeguarding networked information, see *id.*

[30] Prosise, *supra* note 12, at 315.

[31] Evans, *supra* note 25, at 472.

cryptography, "a field of applied mathematics/computer science," which is defined simply as "the technique of concealing the contents of a message by a code or a cipher."[32] Encryption uses a cryptographic algorithm[33] to manipulate the data sent, thereby converting it from normal text, or "plaintext," into an encoded or encrypted form known as "ciphertext."[34] Decryption is just the opposite; it is the process by which encrypted data is translated back into a form the recipient can use.[35] Most encryption methods require the user to have a unique "key" to encrypt and decrypt the message.[36]

Several kinds of encryption methods exist.[37] One method is a symmetric, or single-key, system in which the message is encrypted and decrypted using the same key.[38] Conversely, the public-key, or asymmetric system, needs two keys: one to encrypt the message, and a different, but mathematically related, key to decrypt the message.[39] Because of the mathematical complexity involved, the keys can be formulated so that one key can be disclosed to the public—the "public key"—without fear that anyone will calculate the other key, the "private key."[40]

---

[32] OTA, INFORMATION SECURITY, *supra* note 21, at 113. For a more thorough explanation, see *id.* at 112-13. Cryptography also has been defined more basically as "the scrambling of information into an unreadable language that only the intended recipient can understand." David Banisar, *Roadblocks on the Information Superhighway*, 41 FED. B. NEWS & J. 495, 496 (1994).

[33] Cryptographic algorithms are the "specific techniques for transforming the original input into a form that is unintelligible." OTA, INFORMATION SECURITY, *supra* note 21, at 113.

[34] *See Communications and Computer Surveillance, Privacy and Security: Hearing Before the Subcomm. on Technology, Environment and Aviation of the Comm. on Science, Space, and Technology*, 103d Cong., 2d Sess. 41 (1994) [hereinafter *Hearing*] (statement of Raymond G. Kammer, Deputy Director of the U.S. Department of Commerce, National Institute of Standards and Technology); Lance J. Hoffman et al., *Cryptography Policy*, COMM. ACM, Sept. 1994, at 109, 109.

[35] Prosise, *supra* note 12, at 315.

[36] This "key" is a "sequence of bits" that is "input to the algorithm to successfully perform the desired conversion." Hoffman et al., *supra* note 34, at 109.

[37] For a detailed description of the different types of encryption methods and exactly how they work, see Prosise, *supra* note 12, at 315-21. *See also* James Fallows, *Open Secrets*, ATLANTIC MONTHLY, June 1994, at 46, 46-48 (explaining history and principles of encryption).

[38] *See* OTA, INFORMATION SECURITY, *supra* note 21, at 37, 39. In order to work, both the sender and receiver must know what the key is; this is the single key system's greatest weakness because communications will be secure only as long the key is kept secret. *Id.* at 37, 39; Prosise, *supra* note 12, at 316.

[39] *See* OTA, INFORMATION SECURITY, *supra* note 21, at 38-39; Prosise, *supra* note 12, at 321.

[40] For a basic explanation, see OTA, INFORMATION SECURITY, *supra* note 21, at 38. If *A* wants to send *B* an encrypted message, *A* encrypts the message using *B*'s public key; and *B* then decrypts the message using *B*'s private key. *Id.* The security of this

"The strength of an encryption scheme is dependent both upon the strength of its algorithm and, often, on the length of the keys used for encryption and decryption."[41] Although not the sole factor, the general notion is the longer the key, the stronger the algorithm, because a person requires more time to find a particular key through a "brute force" attack.[42]

The government's need for secure communications is obvious, but encryption also has many uses for both industry and private individuals. In the financial arena, encryption is vital for "cash management and electronic funds transfer services, securities trading and transfer, remote banking, personal identification number transfers and communication of highly sensitive business data."[43] Furthermore,

> [i]t can be used to protect the integrity and/or confidentiality of phone calls, computer files, electronic mail, electronic medical records, tax records, corporate proprietary data, credit records, fax transmissions and many other types of electronic information. . . . Encryption . . . protects the individual privacy of our citizens including, for example, their records and transactions with government agencies and financial institutions. Private sector organizations can also benefit from encryption securing their product development and marketing plans . . . . It can also protect against industrial espionage by making computers more secure against unauthorized break-ins, and if data is encrypted, making it useless for those without the necessary key.[44]

As technological use and capabilities have grown, so has the reliance on strong encryption. Encryption is more than just a benefit of new technological knowledge. In many areas—especially government communications and financial transactions—encryption is a necessity.

---

method of encryption depends on the private key remaining secret and the public key's authenticity. *Id.*

[41] Hoffman et al., *supra* note 34, at 109; *see also* OTA, INFORMATION SECURITY, *supra* note 21, at 113.

[42] OTA, INFORMATION SECURITY, *supra* note 21, at 122. A "brute force" attack consists of using a computer to try every possible key until the actual key is found. *Id.*

[43] Wayne Madsen, *Clinton Approves Clipper, Fails to Relax Export Controls*, COMPUTER FRAUD & SECURITY BULL., Apr. 1, 1994, *available in* WESTLAW, 1994 WL 2299724, COMFSBL Database.

[44] *Hearing*, *supra* note 34, at 41 (statement of Raymond G. Kammer, Deputy Director of the U.S. Department of Commerce, National Institute of Standards and Technology).

D. *Government Policy Considerations of Strong Encryption*

The debate is not whether encryption should be used, but rather what *type* of encryption to use. This debate "is, in many ways, the continuation of an ongoing discussion in the U.S. about the proper balance between national security and individual freedom of action."[45] The government will continue to rely on encryption "to protect its secrets as well as the personal and proprietary data it maintains."[46] The current standard, Data Encryption Standard (DES),[47] a very strong encryption method, "became the de facto U.S. government-approved cryptosystem."[48] Many are convinced, however, that DES is nearing the end of its useful life, and that it will not be secure ten years from now.[49] Because DES is not expected to remain secure much longer, it is necessary to find a new standard, and to minimize any of the accompanying threats from future strong encryption. These threats are often separated into two basic concerns: domestic law enforcement, and national security.[50]

Although the concerns of domestic law enforcement and national security are not identical, they arise out of a common problem—the worldwide proliferation of strong encryption products. DES first became the United States standard, and subsequently became the international standard, especially within foreign financial communities.[51] In addition, foreign manufacturers also provide many strong encryption products. One count puts the number of foreign encryption products at 394, over 150 of which use DES-strength encryption.[52] Although export controls remain on strong encryption, all of these products can be legally imported into the United States.

---

[45] Hoffman et al., *supra* note 34, at 114.

[46] *Hearing*, *supra* note 34, at 46 (statement of Raymond G. Kammer).

[47] DES is a single-key encryption system developed by IBM, and adopted as the federal standard in 1976. It was to be reviewed every five years, and was last reaffirmed as a federal standard in 1993. The prevailing wisdom is that DES will not be reaffirmed in 1998. *See* OTA, INFORMATION SECURITY, *supra* note 21, at 121-23; Prosise, *supra* note 12, at 321.

[48] Prosise, *supra* note 12, at 321. "A cryptosystem is a set of rules that define how data is to be encrypted and decrypted." *Id.* at 315 (emphasis omitted).

[49] Hoffman et al., *supra* note 34, at 110 (noting further that scientists believe that DES may be able to be cracked by "brute force").

[50] Because these spheres share common concerns relating to strong encryption, analysis of their concerns often involves unified treatment. Nevertheless, because the concerns are not identical, they are analyzed separately, *infra*.

[51] Hoffman et al., *supra* note 34, at 110.

[52] Vic Sussman, *Policing Cyberspace*, U.S. NEWS & WORLD REP., Jan. 23, 1995, at 54, 58.

An example of the government's interest in controlling strong encryption programs is represented by the dissemination of the program Pretty Good Privacy (PGP), which was designed in 1991 by Philip Zimmerman. When he learned of a possible government ban on cryptography, Zimmerman gave copies of the program to friends.[53] The program eventually found its way to the Internet, and is now available to anyone worldwide. As a result, PGP has become the "cryptography of the people."[54] This is a particularly vexing development for the United States government, because PGP is so strong that the National Security Agency (NSA) allegedly cannot crack it.[55]

The main domestic law enforcement organization concerned with encryption is the FBI, whose primary focus is "investigating serious crimes and thwarting domestic terrorism."[56] Digital communications and encryption make it difficult, if not impossible, for law enforcement agencies to use wiretaps to intercept and understand communications.[57] When communications are digitized, a wiretap does not intercept a complete conversation, but instead intercepts packets of information that might contain signals from thousands of different conversations.[58] Encryption adds to this problem because it scrambles the electronic communications. The combination of digitalization and encryption results in wiretaps that produce unintelligible partial conversations.

The FBI fears that digitalization and encryption will render wiretapping ineffective, and that as a result "the country [will] be unable to protect itself

---

[53] *See* Levy, *supra* note 11, at 60.

[54] *See id.* As a result of this turn of events, Zimmerman was investigated for alleged violation of the export regulations, which require a license for exporting strong encryption. Steven Levy, *The Encryption Wars: Is Privacy Good or Bad?*, NEWSWEEK, Apr. 24, 1995, at 55, 55. After three years, the government recently dropped its investigation of Zimmerman, although officials have not explained why. Doug Abrahms, *U.S. Drops Probe of Computer Programmer Encryption Software Distributed on Internet*, WASH. TIMES, Jan. 23, 1996, at 36.

[55] *See* Levy, *supra* note 54, at 56.

[56] Hoffman et al., *supra* note 34, at 114.

[57] Grosso, *supra* note 2, at 485. In response to the increased difficulty in wiretapping due to digital communications, the U.S. Department of Justice submitted Digital Telephony legislation to Congress, designed to force telephone companies to improve their communications to make wiretapping easier. *See* H.R. 4922, 103d Cong., 2d Sess. (1994); Grosso, *supra* note 2, at 486. Congress has since passed the Act. *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 104-414, 108 Stat. 4279 (1995) (codified in scattered sections of 18 U.S.C. and 47 U.S.C.); Sussman, *supra* note 52, at 58. Many of the same arguments that have been leveled at the Digital Telephony controversy are parallel to those against encryption. For an examination of the First Amendment implications of the Digital Telephony legislation, see Jaleen Nelson, *Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and Its Effect on Free Flow of Information and Privacy*, 41 UCLA L. REV. 1139 (1994).

[58] Grosso, *supra* note 2, at 486.

against foreign threats, terrorism, espionage, violent crime, drug trafficking, kidnapping and other crimes."[59] At a hearing before the House Subcommittee on Technology, Environment, and Aviation, FBI Special Agent in Charge James Kallstrom predicted dire consequences if law enforcement could not effectively wiretap:

> I can assure you that a loss or diminishment of electronic surveillance will produce the following disastrous results: An increase in loss of life, attributable to law enforcement's inability to prevent terrorist acts and murders. An increase in corruption and economic harm to business, industry, labor unions, and society generally . . . . An increased availability of much cheaper narcotics and illegal drugs—along with the personal, societal, and economic harm brought about by increased drug use . . . . A substantial increase in undetected and unprosecuted violent crimes . . . .[60]

Kallstrom also noted that between 1982 and 1992, court-authorized surveillances resulted in more than 22,000 convictions.[61] He then argued that while undoubtedly useful, wiretapping is not a casual undertaking by law enforcement agencies. Kallstrom observed that only 919 wiretap orders were obtained by all federal, state, and local law enforcement agencies in 1992.[62] Thus, although officials do not wiretap often, they want to ensure that when they do, they can immediately understand what has been intercepted.

In terms of national security considerations, the most powerful player in this debate is the NSA, the federal agency primarily responsible for establishing and operating an effective unified organization for signals intelligence activities.[63] The NSA's activities include "decoding the signals of foreign governments, collecting information for counterintelligence purposes, and conducting research and development into signals intelligence and com-

---

[59] *Hearing*, *supra* note 34, at 16 (statement of James K. Kallstrom, Special Agent in Charge, Special Operations Division, New York Field Division, Federal Bureau of Investigation). Kallstrom listed examples in which wiretapping was important to preventing crime and conducting investigations. *Id.* at 16-18 (statement of James K. Kallstrom).

[60] *Id.* at 18-19 (statement of James K. Kallstrom). Some would argue that these consequences are exaggerated. *See* discussion *infra* notes 256-84 and accompanying text. For an example of such a crime, see Stephen Rodrick & Vladimir Edelman, *Cyberstoned*, MINNEAPOLIS-ST. PAUL STAR-TRIB., May 22, 1995, at 10A (interviewing a drug dealer doing business over the information superhighway).

[61] *Hearing*, *supra* note 34, at 16 (statement of James K. Kallstrom).

[62] *Id.* (statement of James K. Kallstrom).

[63] Evans, *supra* note 25, at 478.

munications security."[64] Furthermore, the NSA is involved in the regulation and control of cryptography.[65] Notably, the NSA only intercepts communications between the United States and other countries, or within foreign countries; it is *not* authorized to intercept domestic communications.[66]

Clinton Brooks, Special Assistant to the Director of NSA, also addressed the House Subcommittee. In his statement, Brooks explained that the NSA's intelligence mission depends on its ability to collect and understand foreign communications, and that encryption can disrupt its foreign signals intelligence operations.[67] This argument appears to be similar to that advanced in the name of domestic law enforcement: that is, if communications were encrypted, the NSA could not discover or prevent terrorist activities.[68] Beyond this argument, the NSA has not offered an explanation for its objections to encryption. Further, the NSA has not explained the "disruption" that encryption allegedly causes.[69] Raymond Kammer, Deputy Director of the National Institutes of Standards and Technology (NIST), offered this vague explanation to the House Subcommittee: "Encryption use worldwide affects our national security. *While this matter cannot be discussed in detail publicly without harm to this nation's intelligence sources and methods*, I can point to the Vice President's public statement that encryption has 'huge strategic value.'"[70] One suggestion has been that the NSA is concerned that its control of the encryption field has eroded due to an increase in the number of devices under development by private firms and individuals.[71] Although unconfirmed, the NSA seems to have two concerns: first, that encryption will hinder signals intelligence, and second, that the NSA will lose its role as the primary source of cryptography.

II. GOVERNMENT ATTEMPTS AT CONTROLLING ENCRYPTION

Due to the proliferation of strong encryption and the corresponding concerns for law enforcement and national security, the federal government seeks to control what it perceives as an ominous threat. The federal

---

[64] *Id.*

[65] *Id.*

[66] Levy, *supra* note 11, at 49.

[67] *Hearing*, *supra* note 34, at 34 (statement of Dr. Clinton C. Brooks, Special Assistant to the Director, National Security Agency). This statement was made in response to the debate over export controls on encryption, a subject more thoroughly discussed *infra* notes 72-75, 129-35, and accompanying text.

[68] Hoffman, et al., *supra* note 34, at 114.

[69] Evans, *supra* note 25, at 487 (noting that some in the software industry have tried to determine the source of disruption caused by encryption).

[70] *Hearing*, *supra* note 34, at 47 (statement of Raymond G. Kammer) (emphasis added).

[71] Hoffman et al., *supra* note 34, at 114.

government's actions in the areas of the export controls imposed on strong encryption, its adoption of the Escrowed Encryption Standard (EES) as a voluntary standard, and, arguably, its attempts to constructively mandate EES by making it the de facto standard for the United States, provide strong evidence that the government will not leave encryption in the hands of private individuals or companies. This section will examine the government's attempts to control encryption, and the responses to those attempts both from the public and from private industry.

A. *Export Controls*

Distribution of strong encryption outside of the United States is strictly governed by export controls.[72] "U.S. export controls policy continues to categorize many encryption items as 'munitions-related,' thereby subjecting them to applicable export laws."[73] Accordingly, exportation of strong encryption requires a license. The licensing procedure includes a thorough review of the application by the NSA.[74] Export controls on encryption are arguably designed to have several effects on the spread and use of technology: first, export controls limit the availability of strategic encryption; second, the controls limit availability of strong encryption which would hinder the NSA's signals intelligence; third, they slow the use of encryption; and fourth, they allow the NSA to assess commercially available encryption.[75]

B. *Adoption of the Escrowed Encryption Standard (EES)*

The recognized need for strong encryption, coupled with the fear of its misuse, led the Clinton Administration to approve the adoption of a new encryption standard.[76] After a period of review and hearings, Escrow En-

---

[72] This subject has been written on extensively, and therefore will be treated here only briefly. For a detailed analysis, see Evans, *supra* note 25. Cryptography can fall under the Arms Export Control Act and International Traffic in Arms Regulations (ITAR) administered by the State Department, or it may come within the Export Administration Act (EAA) or Export Administration Regulations (EAR), administered by the Commerce Department. For a more precise description of how cryptography fits within current regulations, see OTA, INFORMATION SECURITY, *supra* note 21, at 150-54.

[73] Hoffman et al., *supra* note 34, at 113. Recently, these regulations have come under fire, and several lawsuits have been filed challenging the application of the cryptography regulations. *See* discussion *infra* notes 221-23 and accompanying text.

[74] Hoffman et al., *supra* note 34, at 113. This includes exporting products utilizing DES, which is already available throughout the rest of the world. *Id.*

[75] Evans, *supra* note 25, at 488.

[76] *See* White House, Office of Press Secretary, Press Release on 'Clipper Chip' Encryption Initiative, Apr. 16, 1993, *available in* WESTLAW, 1993 WL 357773, PRES-DAILY Database [hereinafter Press Release].

cryption Standard (EES), was formally adopted on February 4, 1994 as a voluntary government standard.[77] The standard was approved to protect sensitive but unclassified data telecommunications, including voice, facsimile, and computer information communicated in a telephone system.[78] The standard is applicable to, but not mandated for, all federal departments and agencies and their contractors; EES is voluntary for the private sector.[79]

EES is a single-key encryption method[80] which utilizes an algorithm known as SKIPJACK and a Law Enforcement Access Field (LEAF).[81] Unlike many methods that are available as software, these two items are encoded into an electronic device or chip, which is then physically implanted in the particular device used, such as a telephone, fax machine, or computer.[82] This encryption standard is commonly known as the "Clipper Chip."

The most controversial aspect of EES is its "key escrowing" feature. Each chip is programmed with the algorithm, an identification number unique to that chip, and a "unique key," which allows the communications to be encrypted.[83] At the time of programming, the unique key is split into two unrelated halves. Each half is held in escrow by separate escrow agents.[84] One half of the key is held by NIST and the other half by the Automated Systems Division of the Treasury Department.[85] The key escrow feature allows law enforcement officials to decipher encrypted communications they intercept pursuant to a wiretap, provided that the message was encrypted using EES.[86] When faced with communications that have been encrypted with EES, law enforcement officials can then obtain the two halves of the key from each of the escrow agents and decrypt the message.[87]

---

[77] Escrowed Encryption Standard (EES), 59 Fed. Reg. 5997, 6003 (1994). This standard became effective March 11, 1994. *Id.*

[78] *Id.*

[79] *Id.*

[80] *See* discussion *supra* note 38 and accompanying text.

[81] Escrowed Encryption Standard (EES), 59 Fed. Reg. at 6003.

[82] *Id.* The chip is also designed to prevent reverse engineering; attempting to take the chip apart to learn how it works results in the destruction of the chip. *Id.*

[83] *See* Geoffrey R. Greiveldinger, *Digital Telephony and Key-Escrow Encryption Initiatives*, 41 FED. B. NEWS & J. 505, 508 (1994). For the technical explanation, see Escrowed Encryption Standard (EES), 59 Fed. Reg. at 5997.

[84] Greiveldinger, *supra* note 83, at 508.

[85] *Id.*

[86] If agents encounter unintelligible communications, they run the communications through a decrypt processor, which can tell them first, whether key escrow encryption is being used, and second, the unique identification number of the chip. *Id.* at 508. The technical explanation of exactly how this is done involves the Law Enforcement Access Field (LEAF) creation method that is implemented in every chip. *See* OTA, INFORMATION SECURITY, *supra* note 21, at 64-65.

[87] When requesting the key components, agents must: (1) identify themselves and their agency; (2) certify that they are conducting a lawful wiretap; (3) specify the

The EES standard was publicized as the best of all worlds.[88] First, it provides the government and the private sector with a strong encryption method. The SKIPJACK algorithm, developed by the NSA, is reportedly sixteen million times stronger than DES, the current standard.[89] Second, EES allows government officials to decipher intercepted communications, thereby furthering the goals of law enforcement and national security. Third, security and privacy are maintained because the key components are unrelated, so knowledge of one half of the key does not provide the ability to determine the complete key.[90] Fourth, each half of the key is itself encrypted, so that even the escrow agents do not see their respective halves in their decrypted form.[91] Finally, strict procedures must be followed before the two halves of the key are disclosed.[92]

C. *Government Attempts to Constructively Mandate EES: Forcing a De Facto Standard*

When it approved the adoption of EES, the federal government announced that the standard was voluntary, and that it would remain so.[93] In his prepared statement before the House Subcommittee, Deputy Director Kammer reaffirmed the Administration's earlier position that it "would not be seeking legislation to restrict the use, manufacture, or sale of encryption products in the U.S."[94] Nevertheless, even accepting that the current Administration will not change its position on this point, and assuming that any future Administration would follow a similar "hands off" approach, the government could undertake certain actions to ensure that EES would eventually become "either the only device or the predominant device available on the market."[95] Thus, government could aid the process by which EES

---

source of the wiretap authority and the termination date; and (4) provide the chip identification number. *Id.* In addition, a government attorney involved in the matter must confirm that a wiretap has been lawfully authorized. Greiveldinger, *supra* note 83, at 508.

[88] *See* Press Release, *supra* note 76.

[89] Greiveldinger, *supra* note 83, at 508. Part of this difference in strength is due to the fact that SKIPJACK is an 80-bit algorithm whereas DES has 56 bits, but the actual strength of SKIPJACK is unknown, because the government has kept it classified. OTA, INFORMATION SECURITY, *supra* note 21, at 118 n.7.

[90] Greiveldinger, *supra* note 83, at 508.

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Hearing*, *supra* note 34, at 47 (statement of Raymond G. Kammer, Deputy Director, U.S. Department of Commerce, National Institute of Standards and Technology).

[95] Hoffman et al., *supra* note 34, at 112 (citing Dorothy Denning, Georgetown University professor and one of the most notable advocates of EES).

"naturally" becomes the accepted standard without actually mandating EES or outlawing the use of any other encryption method. Three areas of government activity arguably illustrate why EES could not be considered truly voluntary: first, the government's adoption of EES as a federal standard; second, the government's attempts to influence the encryption market; and third, remaining export controls on encryption. Although such activities do not constitute an overt mandate, they do signal the government's intent to control the availability and use of strong encryption.

By adopting EES as a federal standard, the government took the first step toward making EES the de facto standard. By their nature, standards allow products to work together more easily and at a lower cost. Further, standards serve to provide predictability in the market.[96] This is especially important in networks in which a need for compatibility is great.[97] Therefore, even weak encryption could gain acceptance in the market and become the de facto standard simply because more people are using it. In this scenario, individuals would still be able to use strong encryption, but the number of people they could communicate with would be small.[98] As a result, "people who buy a nonstandard system might find themselves with an untappable phone but no one to call."[99]

The government also intended to influence the encryption market through its purchasing power. By utilizing its market power, the government could arguably drive down the cost of EES and give it a head start on becoming the global standard.[100] The government was forthcoming about such plans for EES: "NSA has stated numerous times that, through government procurement, it expects to create a large enough market to make Clipper a de facto standard."[101] There also were reports that the government would require the installation of EES as a condition for awarding contracts,[102] a notion confirmed by Deputy Director Kammer.[103]

---

[96] OTA, INFORMATION SECURITY, *supra* note 21, at 46.

[97] *See id.* at 47.

[98] *See generally id.* at 47; Hoffman et al., *supra* note 34, at 116.

[99] Philip Elmer-Dewitt, *Who Should Keep the Keys?*, TIME, Mar. 14, 1994, at 90, 91.

[100] Grosso, *supra* note 2, at 486.

[101] Banisar, *supra* note 32, at 499. For example, as of September 1994, the Justice Department had reportedly ordered 8000 phones installed with the EES chip, and the Department of Defense was believed to have ordered 20,000 chips. Murray Slovick, *The Big Brother Chip*, POPULAR MECHANICS, Sept. 1994, at 116, 117.

[102] *See* Sharon Begley et al., *The Code of the Future*, NEWSWEEK, June 7, 1993, at 70, 70; Jon Healey, *Clinton Pushes Clipper Chip over Industry Objections*, 1994 CONG. Q. 796, 798.

[103] *Clinton Approves Use of Electronic Privacy Standard*, COMM. DAILY, Feb. 8, 1994, *available in* WESTLAW, 1994 WL 2317033, COMMD Database (stating that agencies would be able to require the use of Clipper-installed devices in contract proposals).

Finally, the government maintains its export controls on strong encryption, *except for those companies wishing to export EES.*[104] Other, mass-market software with encryption capabilities could be exported under a blanket license only if the key size was no more than forty bits.[105] By making EES easier to export, the government hoped EES would be favored by manufacturers and quickly replace DES as the encryption standard.

Given the government's attempts to influence the market, the need for compatibility, and the export controls placed on strong encryption, the idea that EES is a truly voluntary standard is tenuous. EES officially was designated as "voluntary," but the actions of the government appear to signal that EES would not be voluntary if the government could have its way.[106] Perhaps Steven Levy phrased the issue best when he asked:

> The Government's stated intent is to manipulate the marketplace so that it will adopt an otherwise unpalatable scheme and make it the standard. Existing systems have to cope with export regulations and, now, incompatibility with the new Government Clipper standard. *Is it fair to call a system voluntary if the Government puts all sorts of obstacles in the way of its competitors?*[107]

D. *Response to EES*

Despite the publicity of EES as the answer to everyone's concerns, the response to EES has been extremely unfavorable. In March 1994, a *Time/CNN* poll showed eighty percent of the 1000 people polled opposed the proposal.[108] Computer Professionals for Social Responsibility organized

---

[104] *See* Rochelle Garner, *Clipper's Hidden Agenda*, UNIXWORLD'S OPEN COMPUTING, Aug. 1, 1994, at 51, 51; Hoffman et al., *supra* note 34, at 114.

[105] Hellman, *supra* note 13, at 28. By contrast, DES has a key that is 56 bits in length. The export requirements were revised sometime in August, 1995. *See* discussion *infra* notes 139-141 and accompanying text.

[106] In fact, through the Freedom of Information Act, the Electronic Privacy Information Center recently obtained FBI documents which advised mandating government-approved encryption, and prohibiting cryptography that does not meet government standards. *See* Kennedy Maize, *FBI Documents-Clipper Must Be Mandatory*, NEWSBYTES NEWS NETWORK, Aug. 23, 1995, *available in* WESTLAW, 1994 WL 2420642, ALLNEWS Database. Scanned images of some of the documents are available online at http://www.epic.org/crypto/ban/fbi_dox.

[107] Levy, *supra* note 11, at 51 (emphasis added).

[108] Banisar, *supra* note 32, at 498-99. Jerry Berman, in his address before the House Subcommittee on Technology, Environment, and Aviation, outlined the main arguments against EES. *Hearing*, *supra* note 34, at 62-73 (statement of Jerry Berman, Executive Director, Electronic Frontier Foundation). Steven Levy presented a somewhat more

an electronic petition against EES which gathered 50,000 signatures, and when NIST issued a public notice in July 1993 asking for public comment on the EES proposal, they received 300 responses, only two of which were favorable.[109] Adopting EES as a standard sparked a fierce debate, with one White House technology official calling it "the Bosnia of telecommunications."[110]

1. *Concern for Privacy*

Most of the opposition to EES is based on the fear that people are giving up their right to privacy by allowing an encryption method with a back door for law enforcement.[111] Advocates of this argument see EES and the Digital Telephony legislation[112] as the first step toward "Big Brother" as envisioned by George Orwell's *1984*. Opponents of EES further argue that the information superhighway will become virtually inescapable; as members of society, people will have no choice but to conduct their personal and business affairs electronically. Arguably, making the information superhighway so wiretap-friendly will turn the system into "a universal surveillance machine,"[113] or the "Information Snooperhighway."[114] These arguments ignore the strict safeguards that are undertaken to keep the keys secret, and the measures that must be taken before officials can obtain the keys.[115]

The issue of safeguards and security measures signals another major privacy concern. Many people simply do not trust the government to keep the keys secret, regardless of the promised security measures. Critics of EES simply do not accept the government rhetoric that the keys will be kept safe from spies, bribes, or fraud.[116] For example, intricate safeguards have been enacted, but there is no provision for sanctions if these safeguards are violated; in fact, each procedure has a *disclaimer* of responsibility.[117] In short,

---

balanced view, but covers most of the arguments levied against EES. Levy, *supra* note 11, at 44, 46.

[109] Banisar, *supra* note 32, at 498-99.

[110] Levy, *supra* note 11, at 51 (quoting Michael R. Nelson).

[111] This argument has been debated many times over, in all types of media. Only the basic issues will be covered here. *See* discussion *infra* notes 151-57 and accompanying text.

[112] For a discussion of the Digital Telephony legislation, see *supra* note 57.

[113] Grosso, *supra* note 2, at 486.

[114] Sussman, *supra* note 52, at 58.

[115] For the opposite view—why EES would violate the Fourth Amendment—see discussion *supra* part III.A.1.

[116] Garner, *supra* note 104, at 54.

[117] Banisar, *supra* note 32, at 498-99 (reprinting the disclaimer: "These procedures do not create, and are not intended to create, any substantive rights for individuals intercepted through electronic surveillance, and *noncompliance with these procedures shall*

there is *no provision for legal liability* in the event of unauthorized release of keys.[118] Moreover, the NSA could easily breach the system, because they are not required to get a wiretap if "national security" is at stake, or for the interception of calls between or within foreign countries.[119] Finally, the bodies chosen to be the escrow agents, the NIST and the Treasury Department, are both part of the executive branch of the federal government, contrary to the United States's system of checks and balances.[120]

2. *Banking and Financial Industry's Concerns*

EES also faced opposition from the financial industry, which arguably has the greatest need for strong, effective encryption. Within international banking and financial institutions, two very strong encryption methods, DES and RSA,[121] have long been the standards. As such, financial officers were reluctant to replace those algorithms with EES.[122]

3. *Concerns Over the Effectiveness of EES*

Initially, there were two areas of concern regarding EES's effectiveness: how well the system worked technically, and whether it would accomplish the government's objectives. Much of the industry's concern about EES is due not only to the fact that the SKIPJACK algorithm was developed in

---

not provide the basis for any motion to suppress or other objection to the introduction of electronic surveillance evidence lawfully acquired.") (emphasis added) (citation omitted).

[118] *Hearing*, *supra* note 34, at 64 (statement of Jerry Berman, Executive Director, Electronic Frontier Foundation).

[119] *See* Banisar, *supra* note 32, at 499; Sussman, *supra* note 52, at 69, 71; *see also* Garner, *supra* note 104, at 51 (arguing that the NSA and CIA have a less rigorous procedure than law enforcement agencies).

[120] Garner, *supra* note 104, at 54.

[121] DES is discussed *supra* note 47. RSA, the Rivest-Shamir-Adleman system, is the best known public-key cryptosystem, allegedly so secure that it would take the world's fastest computer hundreds or thousands of years to decipher. Prosise, *supra* note 12, at 321.

[122] Garner, *supra* note 104, at 54-55. In fact, the vice president of a New York-based bank was quoted as saying that they would use whatever method the government wanted when communicating with the Federal Reserve, but would not surrender their current encryption methods for other transactions. *Id.* at 54. Furthermore, the U.S. Council for International Business developed a list of requirements for a flexible international policy on encryption: (1) free choice; (2) open to the public; (3) international acceptance; (4) flexibility of implementation; (5) user key management; (6) key escrow; and (7) liability. *Business Group Gets Specific on Encryption*, NEWSBYTES NEWS NETWORK, Oct. 11, 1994, *available in* WESTLAW, 1994 WL 2420643, ALLNEWS Database. In many instances, EES fails to satisfy the council's requirements.

secret,[123] but that it remains classified.[124] Industry argued that the only way to inspire confidence that the algorithm works as predicted is to turn it loose and let the researchers and cryptography experts outside of NSA try to crack it.[125] The government responded that this would result in individuals being able to use the EES algorithm without the escrow feature, thereby circumventing law enforcement.[126] Public confidence in EES was further eroded by a report that a flaw had been found in the system.[127]

A more persuasive argument is that if EES was truly voluntary, it could not be effective in aiding law enforcement, an important justification for its development and adoption. First, nothing prevents a sender from encrypting a message by some other method either before or after it is encrypted using EES.[128] Under this scenario, key escrow is meaningless because the message will remain in ciphertext. Second, under the voluntary system, individuals may use whatever other encryption method they desire; criminals and others who do not want to be involved with law enforcement simply will not use EES.

4. *Economics*

The global market for encryption products is growing, but due to export controls, United States manufacturers are at an extreme competitive disadvantage.[129] Most other countries do not have such controls on encryption, and their companies are taking control of the global market.[130] Aside from

---

[123] Some have argued that the NSA's actions in designing the algorithm in secret reverses the presumption that setting standards is an open process. Banisar, *supra* note 32, at 499.

[124] Both the SKIPJACK algorithm and the LEAF creation method are classified. Escrowed Encryption Standard (EES), 59 Fed. Reg. 5997, 6003, 6004 (1994).

[125] *See* Banisar, *supra* note 32, at 499 (arguing that "[u]nder traditional standards setting procedure for security, a standard is made public so that a large number of researchers are able to examine it for flaws"); Garner, *supra* note 104, at 52 (noting that "the accepted method of setting an algorithm is to broadcast the code. This way as many mathematicians as possible can pound on it for as long as possible—as in years").

[126] *See Hearing*, *supra* note 34, at 44, 46 (statement of Raymond G. Kammer, Deputy Director of the U.S. Department of Commerce, National Institute of Standards and Technology).

[127] Banisar, *supra* note 32, at 499 (noting that a Bell Labs researcher has discovered a way of modifying messages encrypted with EES, thereby preventing the messages from being decrypted by law enforcement agencies).

[128] *Id.*

[129] *See* Evans, *supra* note 25; *see also* Hoffman et al., *supra* note 34, at 111 (reporting that U.S. data encryption market was $384 million in 1991, and estimated to reach $946 million by 1996. The world market was estimated at $695 million in 1991, and is predicted to reach $1.8 billion by 1996).

[130] U.S. software and hardware manufacturers hold about 75% of the total global

the financial loss, many companies have simply decided not to manufacture encryption technology, while others have decided to "dumb down" the encryption software they sell abroad.[131] Many American companies simply cannot afford to make two versions of the same product—one with strong encryption to be sold only within the United States, and one with weak encryption to be exported.[132] Critics argue that even if export controls were lifted for EES,[133] no foreign purchaser would buy a system in which the United States government holds the keys.[134]

The debate over the value of EES has become volatile: the government sees it as the best of all possibilities, considering the competing policy choices at play, while the private sector and industry see it as the worst alternative—treading on personal liberty and wreaking havoc on economic stability. The worldwide availability of DES and other strong encryption programs has led some to proclaim that it is too late to put the encryption genie back in the bottle. The debate has been nothing if not colorful: NSA Chief Counsel Stewart A. Baker has dismissed the criticisms of EES as "the revenge of people who couldn't go to Woodstock because they had too much trig homework."[135]

E. *Government Loses the EES Battle, but the Encryption War Continues*

The government seems to have already lost a few battles in its effort to make EES the de facto standard for encryption. The government's original plan called for not only the Clipper Chip to protect voice and low-grade data transmissions, but also the Capstone Chip, which was to protect high speed data communications in computer networks.[136] Although EES has been adopted as a voluntary standard for telephone systems, the government has not taken the next step of adopting EES for computer and video networks. In November, 1993, Representative Maria Cantwell (D-Wash.) and Senator Patty Murray (D-Wash.) proposed an amendment to the Arms Export Act that would remove controls on both software and hardware that incorporate encryption.[137] On July 20, 1994, Vice President Al Gore sent

---

market, but only about 50% of the international encryption market. Hoffman et al., *supra* note 34, at 111.

[131] *See generally* Evans, *supra* note 25 at 489; Hoffman et al., *supra* note 34, at 111-13.

[132] *See* Evans, *supra* note 25, at 489-90.

[133] Banisar, *supra* note 32, at 499.

[134] Hoffman et al., *supra* note 34, at 112.

[135] Levy, *supra* note 11, at 70.

[136] *See* OTA, INFORMATION SECURITY, *supra* note 21, at 64-65; Grosso, *supra* note 2, at 486.

[137] OTA, INFORMATION SECURITY, *supra* note 21, at 160; Banisar, *supra* note 32, at 500.

Cantwell a letter that seemed to signal the government's retreat from controlling encryption. In his letter, Gore stated that EES would be limited to telephone systems, and expressed the Administration's intent to cooperate with industry and privacy advocates.[138] With the exception of telephone systems, the government seemingly has backed away from this particular encryption method for computer and video networks.

The government's retreat was all but confirmed by the Clinton Administration's August 1995 announcement that companies would be allowed to export stronger encryption methods.[139] The new scheme allows for exportation of software employing sixty-four bit encryption, as long as a key escrow system is in place.[140] The keys reportedly would be held in escrow by private companies and would be made available to the government under a court order.[141]

Despite these retreats, the government has not yet surrendered completely in its quest. Although EES no longer appears likely to become the de facto standard, the government still intends to control encryption. The government is accepting suggestions for alternatives to EES, but "[o]ne suggestion it will not embrace is inaction. 'Deciding that the genie is out of the bottle and throwing our arms up is not where we're at.'"[142] Therefore, the government is not insisting on EES, but is demanding an acceptable standard that would still require escrowed keys of some sort.[143] Clinton Brooks, in his testimony before the House Subcommittee, acknowledged the need for reliable encryption, but also noted that it would be irresponsible for government to design a system that would alienate law enforcement.[144]

---

[138] Activities that are to be undertaken include presidential studies of the effects of export controls, alternative types of key-escrow systems for computer networks (including key escrow encryption based on unclassified algorithms or software-oriented), escrow system safeguards, use of nongovernment escrow agents, and liability issues. OTA, INFORMATION SECURITY, *supra* note 21, at 172. For an analysis of the different interpretations of Gore's letter, see *Gore Letter on Clipper Chip Prompts Debate over Interpretation*, COMM. DAILY, July 22, 1994, *available in* WESTLAW, 1994 WL 2314110, COMMD Database.

[139] Daniel Pearl, *Encryption-Software Plan Presented Using 'Keys' Held by Escrow Agents*, WALL ST. J., Aug. 18, 1995, at A3.

[140] *Id.* A November, 1995 draft of the government's export criteria for software key escrow encryption products can be found online at http://csrc.ncsl.nist.gov/keyescrow/criteria.txt.

[141] Michelle Quinn, *Encryption Relaxation Gets Mixed Reaction*, S.F. CHRON., Aug. 18, 1995, at E1. A December 1995 draft of the government's criteria for key escrow agents can be found online at http://csrc.ncsl.nist.gov/keyescrow/criteria.

[142] Levy, *supra* note 11, at 70 (quoting an anonymous White House official).

[143] Benjamin Wittes, *The Year in Cyberlaw; The Rapid Development of the Internet Poses Intriguing New Legal Problems, as Well as Possibilities*, LEGAL TIMES, Dec. 26, 1994, at 5.

[144] *See Hearing*, *supra* note 34, at 121 (testimony of Dr. Clinton C. Brooks, Special

More concrete evidence that the government intends to control encryption is found from announced policy rationales. From a logical standpoint, if government intends to assist law enforcement and signals intelligence, it cannot allow the use of strong encryption. Voluntariness is inconsistent with the objectives of the government. The only way to meet these objectives is to make an accessible system mandatory, or criminals will simply use another system.[145] Critics argue that the government's rationale for aiding law enforcement

> assumes that the Mafia, spies, clandestine activities will all use Clipper encryption, full well knowing in advance that their illicit communications would be open for eavesdropping. If NSA and the FBI believe this, it is a contradiction of their 'intelligence' activities. The only users of Clipper under a mandatory standard would be the legitimate, law-abiding communicators who should not normally be targets of Big Brother snooping.[146]

The government responds that most criminals would be unaware of the government's system, or would forget about it.[147] As FBI Special Agent Jim Kallstrom so eloquently stated:

> Thank God most criminals are stupid! If the smartest segment of the population ever went into crime, we would really have a problem. Will some criminals catch on to the system, and buy their encryption from, let's say, Israel? Yes. Will that be a problem? Yes. But it will be a substantially smaller problem than if we didn't do anything.[148]

Kallstrom does not adequately address the problem of voluntariness hindering effectiveness. This attitude may or may not be justified when dealing with garden-variety criminals, but with the emerging danger of hackers and other computer criminals, the idea that they are stupid when it comes to encryption is ludicrous, further proving that an encryption policy must be mandatory if the government hopes to combat these crimes.[149]

Assistant to the Director, National Security Agency).

[145] *See id.* at 66 (statement of Jerry Berman, Executive Director, Electronic Frontier Foundation).

[146] Jack Robertson, *Get Smart on Codes*, ELECTRONIC NEWS, May 31, 1993, at 9.

[147] Fallows, *supra* note 37, at 50.

[148] *Id.*

[149] The FBI itself apparently recognized this argument early on, as it advocated mandatory encryption. *See supra* note 106.

The government's retreat from the adoption of EES aside, its insistence on some type of key escrow, the inconsistency of voluntariness with stated policy objectives, and the fact that export controls have been relaxed only on condition of key escrow, all evidence the government's intent to control encryption. Once another encryption scheme acceptable to the government is developed, the government will most likely try to use the same or similar mechanisms in an attempt to make it the de facto encryption standard. Alternatively, if law enforcement or signals intelligence actually becomes frustrated by encryption, the government may mandate its preferred encryption scheme. This Note assumes a mandatory encryption scheme will result, either through an actual mandated method or through a general requirement of escrowing personal keys, and analyzes the First Amendment implications of government-controlled encryption.

III. FIRST AMENDMENT FREE SPEECH IMPLICATIONS OF GOVERNMENT-CONTROLLED ENCRYPTION

A. *Other Constitutional Objections to Mandatory Encryption*

In order to place in context the free speech issues raised by mandatory encryption, a survey of other objections that have been raised would be helpful. In addition to the social and political arguments levied against EES in particular, and mandatory encryption in general,[150] such a scheme also raises a number of constitutional objections.

1. *Fourth Amendment*

Mandatory encryption, at least in the form of a mandatory key escrow scheme, is most often attacked on Fourth Amendment grounds—that such a scheme threatens individual rights and may constitute an unreasonable search and seizure.[151] Some argue that the existence of the Clipper Chip increases the potential for government abuse and threatens to alter the bal-

---

[150] *See* discussion *supra* part II.D.

[151] The Fourth Amendment provides that

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV; *see, e.g.*, Mark I. Koffsky, Comment, *Choppy Waters in the Surveillance Data Stream: The Clipper Chip and the Particularity Clause*, 9 HIGH TECH. L.J. 131 (1994); Christopher E. Torkelson, Comment, *The Clipper Scheme: How Key Escrow Threatens to Undermine the Fourth Amendment*, 25 SETON HALL L. REV. 1142 (1995).

ance of power between individual rights and law enforcement.[152] Most of the analysis has been through analogy to existing case law in an effort to determine whether mandatory key escrow constitutes a "search" for Fourth Amendment purposes, and if so, whether such a search would be reasonable.[153] One explanation as to why mandatory key escrow may constitute a search is that:

> [a] key is not itself a conversation . . . but the means to decrypt one. Nevertheless, there should be no doubt that absent government action to force disclosure, a properly guarded key to a cryptographic system would be an item of information for which the user would have both a subjectively and objectively reasonable expectation of privacy. Indeed, the entire point of having a cryptographic system is to increase or create privacy. This is especially true in a public-key cryptographic system, in which the private key is never disclosed. A requirement that keys (or the means to decrypt them) be turned over to the government is thus clearly a search or seizure for Fourth Amendment purposes.[154]

As to the reasonableness of such a search, several arguments have been advanced. First, although wiretaps permit secret seizure of a conversation, "[t]he law does not permit the subsequent secret seizure of a record of that conversation."[155] Second, some argue that a mandatory Clipper Chip would violate the Fourth Amendment, in part because the chips would be implanted not upon probable cause, but rather upon an *assumption*, or in the *anticipation* of some *future* crime, a notion directly at odds with the Particularity

---

[152] Torkelson, *supra* note 151, at 1171-75 (arguing that the balance of power will shift to favor law enforcement).

[153] *See generally* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 823-33 (1995) (analyzing whether mandatory key escrow is a search and seizure, and whether a warrant should be required); Henry R. King, Note, *Big Brother, The Holding Company: A Review of Key-Escrow Encryption Technology*, 21 RUTGERS COMPUTER & TECH. L.J. 224, 249-53 (1995) (analyzing whether key escrow would be considered a "search" and whether users would have an "expectation of privacy"); Kirsten Scheurer, Note, *The Clipper Chip: Cryptography Technology and the Constitution—The Government's Answer to Encryption "Chips" Away at Constitutional Rights*, 21 RUTGERS COMPUTER & TECH. L.J. 263, 277-80 (1995) (analyzing exceptions to the Fourth Amendment and their applicability to encryption).

[154] Froomkin, *supra* note 153, at 829.

[155] John Perry Barlow, *A Plain Text on Crypto Policy*, COMM. ACM, Nov. 1993, at 21, 24.

Clause's intention of limiting the scope of authorized searches.[156] Mandatory key escrow raises many of the same constitutional issues as wiretaps, and seems at least to rise to the level of a Fourth Amendment search, although one commentator has suggested that such a scheme resembles a regulatory search, such as employee drug testing, for which no warrant would be required.[157]

2. *Fifth Amendment*

An additional, though less common argument is that mandatory key escrow would violate the Fifth Amendment's privilege against self-incrimination.[158] Requiring users to make their key available to the government is arguably analogous to forcing users to disclose their secrets in advance,[159] or to allowing a possible *waiver* of any future Fifth Amendment privilege.[160] A contrasting view argues that "there have been no Fifth Amendment claims in cases where cryptologists have deciphered messages by using other recorded conversations of the defendant's to develop their decryption scheme."[161] If there is no Fifth Amendment violation under these circumstances, the argument proceeds, then there certainly is no violation where officials are not using *any* prior encrypted conversations—as is the case with key escrow.[162] Finally, some have argued that the Fifth Amendment would not significantly restrict mandatory key escrow because the purpose of such a scheme is to allow the government to retain the capabilities it already has—capabilities that require a warrant before being executed.[163]

3. *First Amendment: Freedom of Association*

Finally, some critics argue that a mandatory key escrow system would violate the First Amendment's guarantee of freedom of association.[164] This

---

[156] Koffsky, *supra* note 151, at 146.

[157] Froomkin, *supra* note 153, at 830-33.

[158] "No person shall . . . be compelled in any criminal case to be a witness against himself . . . ." U.S. CONST. amend. V.

[159] Barlow, *supra* note 155, at 24.

[160] Scheurer, *supra* note 153, at 280-81.

[161] King, *supra* note 153, at 254.

[162] *Id.* at 254-55.

[163] Froomkin, *supra* note 153, at 837-38. In reaching this conclusion, Professor Froomkin performed two analyses: first, in viewing the chip key as a "private paper," and second, analyzing whether chip key or session key (which is tied directly to the encrypted conversation) could be considered "incriminating." *Id.* at 833-38.

[164] "Congress shall make no law . . . abridging . . . the right of the people peaceably to assemble . . . ." U.S. CONST. amend. I.

argument stems from such cases as *NAACP v. Alabama ex rel. Patterson*[165] and *Talley v. California*,[166] wherein the Supreme Court held that requiring disclosure of an organization's members or an individual's identity could violate the First Amendment freedoms of association and speech.[167] Professor A. Michael Froomkin offers a more detailed analysis, noting that anonymity is essential for some associations to survive, and that cryptography makes such anonymity possible.[168] He further explains that mandatory key escrow threatens this anonymity, because such a scheme makes it possible first, to identify both the source and the content of encrypted e-mail, and second, to identify the receiver—"the person to whom the target of the wiretap is speaking."[169] The result of a legal challenge based on freedom of association will probably depend on the outcome of balancing "whether the interests supporting mandatory key escrow are sufficiently great to justify the increased risk of harassment to political dissidents."[170]

B. *First Amendment Free Speech Implications of Mandatory Encryption*

"Freedom of speech" is a deceptively simple concept on its face—one has the right to speak freely without government interference or punishment.[171] When the First Amendment was enacted in 1791, the Framers envisioned protection for the spoken and printed word. The Framers' concept of speech was relatively limited compared to the communication capabilities we take for granted. As new modes of communication emerge and more topics of speech are discussed openly, trying to guarantee this freedom becomes exponentially more difficult. We no longer simply look at what was said, but must focus also on who the speaker is and where the speech took

---

[165] 357 U.S. 449 (1958).

[166] 362 U.S. 60 (1960).

[167] *See* Barlow, *supra* note 155, at 24 (noting that truly private assembly in cyberspace can take place only with some technical means to hide participants); King, *supra* note 153, at 256-57 (following John Perry Barlow's reasoning, and arguing that if non-Clipper encryption methods become illegal, those using the illegal methods will be easier to identify).

[168] Froomkin, *supra* note 153, at 817-18.

[169] *Id.* at 818.

[170] *Id.* at 820. Froomkin adds that a freedom of association challenge to a mandatory key escrow scheme "would increase its chances of success if the challengers could demonstrate that mandatory key escrow closes off a channel of anonymous communication that has no true alternative." *Id.* This same argument is analyzed in more detail in the discussion of mandatory encryption as a content-neutral "time, place, or manner" regulation. *See* discussion *infra* notes 285-305 and accompanying text.

[171] *See* U.S. CONST. amend. I. "Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ."

place, including physical location and medium. With so many contingencies to account for, it is obvious why many commentators consider First Amendment jurisprudence to be as clear as the federal tax code.

Electronic communications only serve to confuse the issues further. Technology has provided a tool by which communications may remain completely confidential without having to meet clandestinely, face-to-face, or rely on the Postal Service. We have the ability to communicate almost instantaneously with people around the world, and yet keep the conversation private through encryption. Nevertheless, controlling encryption while remaining true to freedom of speech is a profound tightrope walk.

In an effort to understand the impact on freedom of speech, this Note will analyze mandatory encryption under traditional First Amendment jurisprudence. Because electronic communications do not fit easily within even the most basic First Amendment principles, the proper starting place for this analysis is to recognize those analytical difficulties. Therefore, without suggesting any new models, this Note will preface the First Amendment free speech analysis by identifying and analyzing these differences. Next, mandatory encryption will be analyzed both as a content-based and a content-neutral regulation. Finally, this Note will examine the possible chilling effect that mandatory encryption would have on the exercise of free speech.

1. *Basic First Amendment Principles and the Analytical Difficulties Posed by Electronic Communications*

a. *Expression*

As a threshold matter, electronic communications are logically seen as a form of expression that is afforded First Amendment protection. Pure verbal oration and the printed word have always been within the realm of First Amendment protection, but over the years other activities have been defined as "speech," thereby receiving similar protection.

Given what has been protected in the past, there is nothing intuitively discomforting about the notion that electronic communications should be afforded the same First Amendment protections that other forms of communication now enjoy. Nevertheless, as Pool noted, the rapid growth of technology will open the floodgates of discourse—an action that most likely will spark a restrictive reaction, at least initially. "The greatest danger in regulating cyberspace, many experts say, may be that this powerful new technology will be misunderstood and crippled in its infancy by overregulation and fear."[172]

---

[172] Vic Sussman, *Policing the Digital World*, U.S. NEWS & WORLD REP., Dec. 6, 1993, at 68, 68.

Perhaps in anticipation of this overregulation, several commentators have affirmatively expressed the applicability of the First Amendment to electronic communications.[173] Nevertheless, application of current law to this new technology remains uncertain. Constitutional experts question the ability of existing law to guarantee full protection to electronic communications. For example, several years ago Harvard scholar Laurence Tribe proposed the idea of a new constitutional amendment:

> This Constitution's protections for the freedoms of speech, press, petition, and assembly, and its protections against unreasonable searches and seizures and the deprivation of life, liberty, or property without due process of law, shall be construed as fully applicable without regard to the technological method or medium through which the information content is generated, stored, altered, transmitted, or controlled.[174]

Thus, the value of expression would not vary according to the location of the discussion. "Although public discourse will shift from physical spaces to cyberspace, its protection under the First Amendment will be equally vital."[175]

b. *Media*

Although "expression" is protected regardless of its mode of transmission, *how much* protection expression is afforded depends on the medium in which it is delivered:

---

[173] As Ithiel de Sola Pool noted more than a decade ago: "the First Amendment applies fully to all media. It applies to the function of communication, not just to the media that existed in the eighteenth century. It applies to the electronic media as much as to the print ones." DE SOLA POOL, *supra* note 1, at 246. More recently, Professor Rodney Smolla explained: "It is clear that the First Amendment guarantee of freedom of expression may be claimed not just for newspapers and other printed publications, but also for motion pictures, radio and television broadcasts, computer databases, and other forms of modern electronic communication, *including those not yet imagined.*" RODNEY A. SMOLLA, SMOLLA AND NIMMER ON FREEDOM OF SPEECH: A TREATISE ON THE FIRST AMENDMENT, § 13.01[2][b] (1994) (emphasis added).

[174] Proposed by Laurence H. Tribe at the "First Conference on Computers, Freedom, and Privacy," *reprinted in* Gregory E. Perry & Cherie Ballard, *A Chip by Any Other Name Would Still Be a Potato: The Failure of Law and Its Definitions to Keep Pace with Computer Technology*, 24 TEX. TECH L. REV. 797, 798 (1993).

[175] Note, *supra* note 5, at 1087.

> Printed material has the most robust constitutional guarantees, giving publishers, writers, and booksellers the right to safely disseminate almost anything without fear of government interference or arrest. Radio and television stations, on the other hand, live in a sticky regulatory web in which licensees are expected to serve the public interest, and "common carriers" like telephone companies are obliged to serve anyone who asks, with almost no limitations on content.[176]

Today, whether expression by way of electronic media is protected depends on both the content and the method of dissemination.[177]

Print enjoys "virtually absolute protection from government restriction."[178] The aim of the drafters of the Constitution was to guard against any system of prior restraints, that is, the need to obtain government approval prior to publication. The disfavor of prior restraints is reflected in the history of the Supreme Court and lower courts. Even when imposed, such restraints do not remain effective for long.[179]

Broadcast media have been subject to the most stringent regulations. The electromagnetic spectrum in which broadcasting operates arguably has a limited physical capacity, therefore only a limited number of frequencies are available for use. This rationale for regulating broadcast media is often referred to as "spectrum scarcity,"[180] and as a result, the Federal Communi-

---

[176] Sussman, *supra* note 172, at 68.

[177] *See* Note, *supra* note 5, at 1069.

[178] *Id.* at 1071. For example, radio and television personality Howard Stern could write whatever he wanted to in his book without fear of censorship or other governmental interference, but was fined by the FCC for saying similar things on the radio. Sussman, *supra* note 172, at 68.

[179] *See, e.g.*, United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979), *dismissed*, 610 F.2d 819 (7th Cir. 1979), which enjoined the publication of an article which described a method of manufacturing a hydrogen bomb. Nevertheless, the restraint was not ultimately successful—before the appeal could be heard, the government dropped the case, because the controversial information subsequently had been printed in other publications. United States v. Progressive, Inc., 610 F.2d 819 (7th Cir. 1979), *dismissing* 467 F.Supp 990 (W.D. Wis. 1979); *see also* New York Times Co. v. United States, 403 U.S. 713 (1971) (per curiam), wherein the government sought to enjoin two newspapers—the *New York Times* and the *Washington Post*—from publishing the so-called "Pentagon Papers", a classified study entitled "History of the U.S. Decision-Making Process on Vietnam Policy." *Id.* at 714. Before the case reached the Supreme Court, the government successfully obtained a prior restraint against the *New York Times*. United States v. New York Times, 444 F.2d 544 (2d Cir.), *rev'd*, 403 U.S. 713 (1971). The Supreme Court reversed the prior restraint. *New York Times*, 403 U.S. at 714.

[180] *See, e.g.*, Red Lion Broadcasting Co. v. FCC, 395 U.S. 367 (1969) (upholding FCC "fairness doctrine" requiring broadcasters to grant individuals a right of reply, due

cations Commission (FCC) is given the authority to license broadcasters.[181] The other prevalent rationale for regulation is that the broadcast media enjoys a uniquely pervasive presence in our lives. In other words, listeners and viewers may not easily be able to avoid the broadcast.[182] Thus, as media becomes more widespread and plays more of a part of our everyday lives, the government is able to regulate it as a matter of public interest.[183]

Telephones, or common carriers, are a different medium from broadcast media. Telephones provide one-to-one interactive communication, rather than one speaker or writer communicating to the multitudes.[184] Furthermore, the First Amendment protects callers' speech,[185] and the telephone companies do not have the right to censor what is transmitted over the lines.[186]

The problem of finding the "right" regulation for these new electronic communications stems from the fact that they do not fit easily within the three traditional classifications of media: print, broadcast, or common carrier.[187] The composition of text and distribution of files over a computer network looks like printing and publishing, but because it is disseminated over the network, it also looks like broadcasting. Also, one can have a one-on-one "conversation" by sending e-mail back and forth, which resembles the interactive element of telephone communications, especially when car-

---

to scarcity of broadcast frequencies).

[181] Note, *supra* note 5, at 1064. Regulation is permitted because "broadcast channels are a scarce public resource and that, in exchange for receiving the exclusive right to exploit such a valuable public commodity, broadcasters should both expect and accept regulation intended to insure that they operate in the public interest." Philip H. Miller, Note, *New Technology, Old Problem: Determining the First Amendment Status of Electronic Information Services*, 61 FORDHAM L. REV. 1147, 1150 (1993).

[182] *See* FCC v. Pacifica Found., 438 U.S. 726 (1978) (upholding FCC's ban on indecent broadcast due to "uniquely pervasive presence" of broadcasting, and its accessibility to children). The pervasiveness rationale attempts to address two concerns: first, that an individual may be confronted with offensive, indecent material in his home, where his privacy interests outweigh the "intruder's" First Amendment rights; and second, that broadcasting is uniquely accessible to children, and broadcasters cannot transmit material to adults without also reaching children. Note, *supra* note 5, at 1078.

[183] For a more in depth discussion of frequency scarcity and pervasiveness, see Note, *supra* note 5, 1070-81.

[184] *Id.* at 1065.

[185] *Id.* at 1086.

[186] Miller, *supra* note 181, at 1160.

[187] For a discussion of how electronic information services ought to be regulated, see *id.* at 1192-1201. This is one area of the law that has some precedent, as a federal district court ruled that an electronic information service, Compuserve, was more like a distributor than a publisher of defamatory statements that appeared in one of its forums, and therefore granted Compuserve's motion for summary judgment. Cubby, Inc. v. Compuserve Inc., 776 F. Supp. 135 (S.D.N.Y. 1991). For a detailed analysis of the court's reasoning in *Cubby*, see Miller, *supra* note 181, at 1194-1201.

ried over telephone lines. Electronic communications challenge media-defined regulations because existing regulations regarding radio and television broadcasting contemplate one-way transmissions, not interactive technology.[188] The two rationales for regulating broadcast media simply do not apply to electronic communications. There is no transmission over public airwaves, so spectrum scarcity is not an issue.[189] Furthermore, electronic communications do not have the same pervasiveness and captive audience problems that broadcast media can have. As an example,

> electronic information services [EIS] would seem to be among the least intrusive of communications media, since gaining access to an EIS requires the use of a considerable amount of computer equipment, a 'dial up' initiated by the user, and (at least for commercial services) the entering of an individual password assigned to each user.[190]

Electronic communications are becoming increasingly common, but for now, a good deal of computer equipment is necessary in order to receive such communications. These facts militate against a finding of pervasiveness.

c. *Identifying the "Speaker"*

With electronic communications, not only is it hard to classify the medium, but with so many aspects of the three traditional classifications blended together, the roles of the people involved are also difficult to label. The interactive element of computer networks merges roles that are at present clearly delineated. The overlapping roles create a new problem of defining who is the "speaker" for First Amendment purposes. Under traditional forms of communication, the identity of the speaker was fairly obvious: it was the person verbally speaking, writing, publishing, or broadcasting. Electronic communications give rise to three possible speakers: network operators, programmers/service providers, and users.[191] The simple idea of a "user" is different from traditional individual speakers and writers:

> Individuals will no longer simply be "viewers" or "receivers" of the electronic media; they will become "users" of it, capable not only of creating their own video, voice, and text

---

[188] Note, *supra* note 5, at 1082.

[189] Miller, *supra* note 181, at 1191-92.

[190] *Id.* at 1192.

[191] For a discussion of how each of these potential speakers will function (compared to current technology and similar roles), and how the First Amendment may be applied to them, see Note, *supra* note 5, at 1084-88.

> messages, but also of communicating them to a large number of others. The convergence of technologies will engender a convergence of roles between system owners, programmers, and users. The communications hierarchy will be replaced with interactivity.[192]

This interactivity available to the user also is the reason that the First Amendment becomes so important. The user is more than simply a speaker; he also has become in essence a writer and publisher. As his interests in freedom logically increase, society also has a higher stake in keeping the discourse free from restrictions. "Indeed, the ability to communicate interactively with a large segment of the public through point-to-multipoint transmissions will reinforce users' First Amendment interests, in part because the speech will contribute to *public* discourse rather than to a merely private conversation."[193] For purposes of First Amendment analysis of encryption, this Note will focus on users as speakers, because they access electronic communications and send messages. Furthermore, the message is encrypted when sent, with the user deciding how to encrypt the message.

d. *Content Categories*

Certain categories of speech receive little or no First Amendment protection, including obscenity,[194] defamation,[195] incitement of imminent lawless behavior,[196] and commercial speech.[197] These categories are consid-

---

[192] *Id.* at 1083.

[193] *Id.* at 1086 (emphasis added).

[194] *See, e.g.*, Miller v. California, 413 U.S. 15, 24-26 (1973) (setting the basic guidelines for determining what is "obscene" as judged by "contemporary community standards"); Roth v. United States, 354 U.S. 476 (1957) (finding no First Amendment protection for obscenity).

[195] Defamation may or may not be defended on First Amendment grounds, depending on who the target of the defamation is, and the subject matter discussed. *See, e.g.*, Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974) (dealing with private figures); Curtis Publishing Co. v. Butts, 388 U.S. 130 (1967) (dealing with public figures); New York Times v. Sullivan, 376 U.S. 254 (1964) (dealing with public officials and criticisms of their official conduct).

[196] *See, e.g.*, Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (holding that a state cannot forbid advocacy of the use of force or law violation except when such advocacy is directed toward inciting imminent lawless action and is likely to incite or produce such action).

[197] Commercial speech receives some First Amendment protection, but it is limited. *See, e.g.*, Posadas de P. R. Assoc. v. Tourism Co., 478 U.S. 328 (1986) (upholding ban on casino advertising aimed at Puerto Rican residents); Central Hudson Gas & Elec. Corp. v. Public Serv. Comm., 447 U.S. 557 (1980) (recognizing commercial speech as being entitled to lesser protection).

ered to have "low" First Amendment value. With the growth of electronic communications, categorizing information will become more difficult, while punishment for communicating information in the unprotected categories will be difficult, if not impossible.[198] One example is obscenity. Possession of obscene materials is permissible in the privacy of one's own home.[199] The electronic transfer of information makes obscenity even more readily available to individuals at home.[200] Therefore, the traditional arguments against obscenity such as accessibility by children, secondary effects on the neighborhood, and offending the sensibilities of the general public no longer apply.[201] Furthermore, defining something as obscene in light of contemporary community standards would be impossible in boundless cyberspace.[202] One cynical argument is that prosecutors will define the standards by filing charges in the most conservative jurisdiction that cyberspace reaches.[203]

Thus, the argument progresses, content regulations will simply be replaced by time, place, or manner regulations, thereby allowing officials to retain some measure of control.[204] In that respect, First Amendment jurisprudence related to electronic communications may change dramatically as the dividing line between content-based and content-neutral regulations is largely erased. Nevertheless, this Note assumes those distinctions remain.

e. *Summary*

Generally, electronic communications add more questions to the already complex freedom of speech jurisprudence. The challenge will be to preserve the utmost freedom for individuals while maintaining order and stability

---

[198] *See* Katsh, *supra* note 13, at 1490-92 (arguing that prior restraint will become impossible, and punishment after distribution will also be difficult).

[199] Stanley v. Georgia, 394 U.S. 557 (1969).

[200] *Cf. id.* Katsh, *supra* note 13, at 1473-75 (discussing how electronic transmission of information has eliminated many of the constraints of previous forms of communication).

[201] Note, *supra* note 5, at 1095.

[202] For example, in July, 1994, a federal jury found a couple guilty of distributing obscene material via a computer bulletin board system (BBS). The case was brought in Memphis, Tennessee, even though the BBS operated in Milpitas, California, near San Francisco; their convictions were affirmed on appeal. United States v. Thomas, 74 F.3d 701 (6th Cir. 1996); *see also* Grosso, *supra* note 2, at 484. The case is controversial because the "contemporary community standards" applied were that of Memphis, not the remarkably different standards of Northern California. Grosso, *supra* note 2, at 484.

[203] For an analysis of this issue, *see* Grosso, *supra* note 2, at 484 (questioning "whether the most restrictive standard of the most conservative community is to become the *de facto* standard for the entire country").

[204] Katsh, *supra* note 13, at 1492. For another analysis on the future of content-based regulations, see Note, *supra* note 5, at 1094-96.

through this technological revolution. Recalling the foregoing definitional complexities, the next section focuses on how mandatory encryption may fare under traditional First Amendment free speech jurisprudence.

2. *Content-Based Versus Content-Neutral Restrictions*

When a government regulation on speech is challenged, the first inquiry is to determine whether the regulation is content-based or content-neutral.[205] "The government's purpose is the controlling consideration in making this decision."[206] A regulation is content-based if the government adopted it because the government disagrees with the *message* being conveyed[207] or if it is aimed at the *communicative impact* of the speech—if it restricts speech because of the specific message conveyed or because of the effects that the speech produces.[208] A content-based regulation is presumed to violate the First Amendment and will be held unconstitutional unless the government can show that the speech falls within one of the categories that receive less protection.[209] Accordingly, the court will decide whether the speech has "low" First Amendment value, like obscenity and commercial speech. If it does not, the speech is given virtually absolute protection absent time, place, or manner restrictions.[210] Laws that are content-based and do not have low First Amendment value generally trigger heightened scrutiny and are almost always struck down.[211]

On the other hand, "[a] regulation that serves purposes unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some speakers or messages but not others."[212] As defined by Laurence Tribe, content-neutral regulations are aimed at the *noncommunicative impact* of the speech.[213] Their enforcement, however, has an adverse effect on communicative opportunity.[214] With content-neutral regulations, courts must balance the competing interests of government and the speaker, and

---

[205] *See* SMOLLA, *supra* note 173, § 3.01[2][b].

[206] Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

[207] *Id.* at 791.

[208] LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW, § 12-2, at 789-90 (2d ed. 1988).

[209] *Id.* § 12-2, at 790-92. Examples of such categories are listed *supra* notes 194-97 and accompanying text.

[210] *See* Tinker v. Des Moines Indep. Community Sch. Dist., 393 U.S. 503 (1969) (holding that ban on wearing black armbands to school in protest of the Vietnam War was not a valid place restriction); TRIBE, *supra* note 208, § 12-3, at 794-95; Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46, 47-48 (1987).

[211] *See* SMOLLA, *supra* note 173, § 3.02[1][a]; Stone, *supra* note 210, at 48.

[212] Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

[213] TRIBE, *supra* note 208, § 12-2, at 790.

[214] *Id.*

only uphold the regulation if it does not unduly constrict the flow of information and ideas.[215] Unlike content-based regulations, content-neutral regulations are subject to an intermediate level of scrutiny, which more often than not results in the regulation being upheld.[216]

3. *Mandatory Encryption As a Content-Based Regulation*

A mandatory encryption scheme facially seems to be content-neutral. Under a mandatory encryption scheme, the government is not singling out what is said, but rather is merely requiring that if a conversation is going to be encrypted that it be done in a particular way. Encryption also does not seem to fall within the realm of "expressive conduct." In *Spence v. Washington*,[217] the Supreme Court found that the appellant had engaged in expressive conduct because "an *intent* to convey a *particularized message* was present, and in the surrounding circumstances the likelihood was great that the message *would be understood* by those who viewed it."[218] With encryption, neither of these elements are present. Accordingly, one could characterize encryption as content-neutral because: (1) encryption is used to keep communications private, not to send any particular message, and (2) the only people who could "perceive" such a "message" would be those who would intercept the encrypted text, which alone does not convey anything to them.

Others, however, argue that in order to properly analyze whether mandatory encryption is content-based, one must focus on the encryption algorithm or the encrypted message, and decide whether either can be considered protectable speech. Accordingly, several commentators have suggested that the encryption algorithm itself is either speech or written expression protectable by the First Amendment. Kate Martin, Director of the American Civil Liberties Union Center for National Security Studies, in addressing the Computer Systems Security and Privacy Advisory Board, remarked that "encryptic communications *and* encryption algorithms are a form of speech protected by the First Amendment."[219] Similarly, John Perry Barlow, a noted commentator on technology law, believes that "the encryption software itself is written expression, upon which no ban may be constitutionally imposed."[220]

---

[215] *Id.* § 12-2, at 791.

[216] SMOLLA, *supra* note 173, § 3.02[1][a], at 3-11.

[217] 418 U.S. 405 (1974) (appellant attached a peace symbol to the front and back of his American flag and hung the flag upside down from his window).

[218] *Id.* at 410-11 (emphasis added).

[219] *Commerce Advisory Board Faces Doubts About 'Clipper Chip' Initiative*, Daily Rep. for Executives (BNA), June 3, 1993, at A-11 (quoting Kate Martin, Director of the ACLU Center for National Security Studies).

[220] Barlow, *supra* note 155, at 24 (noting further that the constitutionality of export

In any event, the courts may ultimately decide the issue. Several cases have been filed challenging the export regulations of encryption, arguing in part that the First Amendment protects the encryption algorithm. In February 1995, a lawsuit was filed in California by a mathematics graduate student who wished to publish the encryption algorithm he developed, along with a paper describing the algorithm and a computer program that runs the algorithm.[221] In part, the lawsuit challenges current export regulations as an impermissible prior restraint on speech, and as a content-based regulation of speech.[222] Additionally, a San Diego software developer is challenging the export regulations which allowed him to obtain an export license for a book on cryptography, but not for a computer disk which contained the same source code listed in the book.[223] The plaintiff, Philip R. Karn, is alleging that the export regulations relating to the disk violate free speech, act as a prior restraint on speech, and chill the exercise of free speech.

Putting aside the protectability of the encryption algorithm, affording First Amendment protection for an encrypted message may call for a new understanding of what is meant by "expression." Considering the problems electronic communications already pose for other areas of First Amendment analysis, perhaps such a redefinition is necessary. A new idea of expression would have to define precisely "messages," and what constitutes the "content" of electronic communications.

The question is whether the protectable message is the plaintext or cyphertext. Anyone can understand plaintext, but cyphertext is the particular bit pattern that results when the communication is sent; that is, the actual arrangement of ones and zeroes that the computer reads. Those who support protecting cyphertext argue that "[t]he process of encryption changes the original message into a coded one by use of an encryption algorithm. . . . Regardless of the method, an encrypted message is a mathematical translation of the original. As a form of communication, it should be considered speech under the First Amendment."[224] Considering cyphertext alone as

---

restrictions simply had not been challenged). There is speculation that government officials dropped their investigation of Phil Zimmerman because they were unwilling to undertake a case that might potentially scrutinize the application of export laws to cryptography. *See* Abrahms, *supra* note 54, at 36.

[221] Bernstein v. United States Dep't of State, No. C95-0582-MHP (N.D. Cal. filed Feb. 21, 1995); *see also* Peter Cassidy, *Cryptography Suit Seeks Definition*, COMPUTER WORLD, Mar. 27, 1995, at 73.

[222] The full text of Bernstein's complaint is available online at http://www.eff.org/pub/Alert/eff_bernstein_950221.complaint.

[223] Karn v. United States Dep't of State, No. 95-CV-01812 (D.D.C. filed Sept. 21, 1995); *see also Crypto Speech Case Heating Up*, INFORMATION LAW ALERT: A VOORHEES REPORT, Dec. 9, 1994. The full text of Karn's complaint can be found online at http://www.qualcomm.com/people/pkarn/export/complaint.html.

[224] King, *supra* note 153, at 255.

the message would render the idea of a content-based regulation completely unworkable. Defining each cyphertext as a different message from the underlying plaintext is the same as saying "der Kater ist weiss," "koshka byela," "le chat est blanc," and "WKHFDWLVZKLWE" are different messages, when they all translate into English as "the cat is white."[225] Following this line of reasoning, in all five cases the "content" would be the different *words* used and their *spelling* instead of the actual *meaning* of the sentence.

Under Tribe's definition, a regulation is content-based if it is aimed at the communicative impact of the speech—the message being conveyed or the effects that the speech produces.[226] Under this definition, mandatory encryption may be considered content-based, depending upon the government's rationale and the classification of the harm that the government is trying to prevent. For example, if the government is trying to guarantee the ability to wiretap effectively, then the regulation appears content-neutral. If, however, the harm to be avoided is criminal solicitation and conspiracy, then the harm is *inherent in the communication itself* and the regulation appears to be content-based, masked as content-neutral. Under this latter analysis, regardless of how the restriction is applied, it is enacted because of *what* is being said and the *reason* for which the transmission lines are being used.[227] The government is afraid that it will not be able to listen to *what people might be saying or planning*. Encryption itself does not threaten national security or safety; it is the *activity* being planned out of the government's sight or hearing that is the threat.

If mandatory encryption is found to be content-based, then a regulation implementing mandatory encryption would have to survive strict scrutiny by the courts. To withstand such scrutiny, the government would have to show that the regulation serves a compelling state interest and is narrowly drawn to achieve that end.[228] In all likelihood, however, most courts would not engage in the mental gymnastics necessary to find a content-based restriction when the more logical option of finding a content-neutral restriction is

---

[225] Under this analysis, the English version would constitute a fifth message. The phrases listed are German, Russian, French, and Caesar cipher, respectively. The Caesar cipher "substitutes every letter in a message with the letter that is three letters higher-A becomes D, B becomes E, and so on." Prosise, *supra* note 12, at 315.

[226] TRIBE, *supra* note 208, § 12-2, at 789-90.

[227] *See* Greiveldinger, *supra* note 83, at 505-06 (discussing drug trafficking and white collar crime).

[228] *See* Widmar v. Vincent, 454 U.S. 263, 269-70 (1981). Whether the state interest would be compelling closely follows the content-neutral "time, place, or manner" analysis. *See infra* notes 239-305 and accompanying text. One commentator has suggested that mandatory key escrow could be viewed as compelled speech, and would be analyzed under this same strict scrutiny. *See* Froomkin, *supra* note 153, at 812-15.

available. Thus, mandatory encryption as a content-neutral regulation is analyzed in more detail.

4. *Mandatory Encryption As a Content-Neutral Regulation*

Apart from the issue of the reason that the government is listening, mandatory encryption more comfortably fits within the content-neutral classification. A regulation is content-neutral if it is justified "'without reference to the content of the regulated speech.'"[229] Nevertheless, content-neutral regulations are not automatically upheld by the courts, regardless of the reasons they were passed, because their *effect* is to reduce the total quantity of speech circulating in society.[230] "Overt censorship of disfavored viewpoints is not the only means of silencing speech; the free flow of information can be reduced by non-content regulation as well."[231]

Under mandatory encryption the government would not pick and choose who can and who cannot use encryption, or define what subject matter could be encrypted using a particular encryption scheme. Mandatory encryption instead would proscribe a particular *means* of communication. The government has recognized the need for strong encryption, and therefore would not ban it outright. Instead, a mandatory encryption scheme would allow encryption only under certain conditions, thereby denying citizens a completely private means of communication. Because mandatory encryption would most likely be considered content-neutral, the court would likely only use intermediate scrutiny.[232] Nevertheless, there are several ways in which the courts may evaluate mandatory encryption's constitutionality.

a. *Incidental Impact Regulations*

The first type of content-neutral regulations are those restricting "symbolic expression," also referred to as "incidental impact" regulations. Although these laws are not passed to regulate the content of the speech, they still incidentally affect speech.[233] When the government attempts to regulate conduct that contains both "speech" and "nonspeech" elements, the regulation will be upheld if it can meet the four-part test set out in *United States v. O'Brien*:[234]

---

[229] Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989) (quoting Clark v. Community for Creative Non-Violence, 468 U.S. 288, 293 (1984)).

[230] SMOLLA, *supra* note 173, § 3.02[1], at 3-12.

[231] *Id.*

[232] Intermediate scrutiny requires that the government have only a "significant" or "substantial" interest in regulating speech. *See id.* § 3.02[3][A], at 3-36 to 3-37.

[233] *See id.* § 3.02 [4][a], at 3-50.

[234] 391 U.S. 367 (1968).

> [A] government regulation is sufficiently justified if it is within the constitutional power of the Government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.[235]

These laws regulate conduct, but they also have an incidental impact on speech because the conduct sought to be restricted conveys a message, or at least is capable of conveying a message. For example, burning draft cards or the American flag is conduct, but that conduct also conveys a message of protest. Therefore, the Supreme Court analyzed laws prohibiting such types of conduct as incidental impact regulations.[236]

Mandatory encryption does not appear to fit the definition of an incidental impact regulation, where representative cases have dealt with conduct capable of conveying a message.[237] Encryption is definitely conduct, but to say that the act of encrypting conveys a message requires quite a stretch in logic.[238] A court probably would be disinclined to follow such logic, given the easier analytical fit of mandatory encryption as a time, place, or manner regulation.

---

[235] *Id.* at 377.

[236] For example, the Court in *O'Brien* upheld the defendant's conviction for burning his draft card, even though he did so to protest the Vietnam War, finding a substantial and legitimate government interest in preventing the destruction of draft cards. *Id.* at 378-80. By contrast, the Court has twice struck down laws against flag desecration, finding that the laws banning such desecration were not designed to further an important governmental interest. Instead, the Court found that the laws were passed because of a disagreement with the speaker's message, which was conveyed by burning the nation's symbol. *See* United States v. Eichman, 496 U.S. 310, 314 (1990); Texas v. Johnson, 491 U.S. 397, 408-10 (1989).

[237] *See* Ward v. Rock Against Racism, 491 U.S. 781 (1989) (holding that New York City's sound amplification guidelines for music programs in Central Park were valid as a reasonable regulation of the place and manner of expression); *see also* Clark v. Community for Creative Non-Violence, 468 U.S. 288 (1984) (holding that sleeping in public parks to dramatize the plight of the homeless was expressive conduct); Tinker v. Des Moines Indep. Community Sch. Dist., 393 U.S. 503 (1969) (holding that wearing black armbands to school in protest of the Vietnam War seen as nearly "pure speech").

[238] *See* discussion *supra* part III.B.3.

b. *Time, Place, or Manner Regulations*

The most common type of content-neutral restriction is a time, place, or manner regulation.[239] With these types of regulations, the government is not concerned with *what* was said, but rather when, where, or how loudly something was expressed.[240] Mandatory encryption fits easily within this description. One useful analogy may be that encrypting communications is like speaking in a language the government cannot understand or translate.[241] Thus, the government is proscribing a certain language or manner of speech.

The location, or forum, in which the speech takes place is an important factor in undertaking a time, place, or manner analysis. The Supreme Court has defined three different categories of forums:

> (1) "traditional" public forums, such as parks, which have historically been dedicated to assembly and debate; (2) "designated" public forums, consisting of public property which the government has opened for use by the public as a place for expressive activity; and (3) "nonforums," places which have not by either tradition or designation been used for indiscriminate expressive activity.[242]

The forum in which the speech takes place determines how much speech regulation the government can employ: the more open and public the forum, the stricter the standards the government must meet.[243]

For the purposes of forum analysis, computer networks are functionally very similar to traditional public forums, in that some computer networks were specifically designed for interactive communication and exchange of ideas on a massive scale.[244] Several differences exist, however, which

---

[239] *See* SMOLLA, *supra* note 173, § 3.02[3][a], at 3-32.

[240] *Id.*

[241] *See* King, *supra* note 153, at 255. "Self styled 'cypherpunks' argue that the government has no more right to insist on a back door in secure telephones than it does to restrict the language or vocabulary used in telephone conversations on the grounds that dialect might hinder interpretation of wiretaps." Paul Wallich, *Clipper Runs Aground*, SCI. AM., Aug. 1993, at 116, 116. As John Perry Barlow explains: "Whole languages (most of them patois) have arisen on this planet for the purpose of making the speaker unintelligible to authority. I know of no instance where, even in the oppressive colonies where such languages were formed, slave-owners banned their use." Barlow, *supra* note 155, at 24.

[242] *See* SMOLLA, *supra* note 173, § 3.02[3][c], at 3-40.

[243] *See* JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW § 16.47, at 1145-48 (5th ed. 1995); SMOLLA, *supra* note 173, § 10.02[1][a]-[c].

[244] *See* Grosso, *supra* note 2, at 481-82.

make the comparison less than perfect. For example, in a computer network, the "speakers" can remain anonymous, out of public view, and can choose how few or many receive their communication. Also, the public does not yet have free access to cyberspace, considering the amount of equipment and cost that may be necessary to access the networks. On the other hand, networks are not controlled by the government and therefore cannot be considered designated public forums. In addition, because their sole function is to facilitate expressive activity, networks cannot be considered nonforums. Logically then, networks are the functional equivalent of the open-air market, with the added feature that this market spans the entire globe. The government can employ a time, place, or manner restriction in a traditional public forum as long as it "promotes an important interest unrelated to the suppression of a particular message and does not unnecessarily restrict the ability to communicate the message."[245]

The Supreme Court has adopted a three-part test to determine whether a time, place, or manner regulation is constitutional. Government may impose restrictions on speech if they "'are justified without reference to the content of the regulated speech, [if] they are narrowly tailored to serve a significant governmental interest, and [if] they leave open ample alternative channels for communication of the information.'"[246] The party challenging the regulation has the initial burden of showing that the regulation impinges on speech. Once that threshold showing is met, which would likely be simple in the case of mandatory encryption, the burden lies with the government to show that the regulation satisfies all three parts of the test.[247]

As previously noted, because mandatory encryption is more accurately described as content-neutral rather than content-based,[248] it easily meets the first prong. The second and third prongs provide more of an analytical challenge.

1. *"Narrowly Tailored"*

With respect to the first half of the second prong, the Supreme Court in *Ward v. Rock Against Racism*[249] reaffirmed that the regulation need not be the least restrictive means available in order to be narrowly tailored.[250] In fact, the Court noted that the requirement would be satisfied if the "regula-

---

[245] *See* NOWAK & ROTUNDA, *supra* note 243, § 16.47, at 1093; SMOLLA, *supra* note 173, § 10.02[a][i]-[iii], at 10-21 to 10-22.

[246] Ward v. Rock Against Racism, 481 U.S. 781, 791 (1989) (quoting Clark v. Community for Creative Non-Violence, 468 U.S. 288, 293 (1984)).

[247] SMOLLA, *supra* note 173, § 3.02[3][d], at 3-50.

[248] *See* discussion *supra* notes 229-32 and accompanying text.

[249] 491 U.S. 781 (1989).

[250] *Id.* at 798 (emphasis added).

tion promote[d] a substantial government interest that would be achieved *less effectively* absent the regulation."[251] Therefore, the Court will not automatically invalidate a regulation just because alternatives exist, but the means chosen must not be substantially broader than necessary to achieve the government's interest.[252]

Without an actual regulation, it is obviously difficult to predict whether mandatory encryption would be narrowly tailored. Whether a regulation would be upheld depends on the exact speech limits imposed and the regulation's impact on users. The crucial focal point becomes what a court would view as most important to the user. If the focus is on the ability to choose among different encryption methods, then mandating one particular encryption scheme for all users of electronic communications can hardly be considered narrow. Different encryption methods are used for different purposes. Therefore, mandating one particular method could impair the ability to encrypt effectively. Mandating key escrow generally, which allows a choice of encryption but which requires that the key be made available to the government should they need it, seems less narrow. An even less restrictive regulation would require escrow of keys of a certain bit length or more, mirroring the government's recent proposal for export decontrol. Under an escrow scheme, however, one would arguably have more choices among encryption methods. The restriction would therefore be narrowly tailored, as long as the industry provides choices. If the government tried to force a de facto standard again, as it did with EES, then the users' choice would be illusory.[253] There would be *no* choice of mandatory encryption that allowed a *completely private conversation.*[254] If the focus is on the users' right to speak privately, then any scheme providing instant access to the government cannot be narrowly tailored.

---

[251] *Id.* at 799 (quoting United States v. Albertini, 472 U.S. 675, 689 (1985)) (emphasis added).

[252] *Id.* at 800.

[253] Mike Godwin, online counsel for the Electronic Frontier Foundation, made this very argument against EES:

> Freedom of choice is meaningful only if there are real choices. The government's export strategy is designed to make sure that there aren't any choices. If commercial software companies aren't allowed to sell encryption to the world market, they're unlikely to develop strong, easy-to-use alternatives to the Clipper. And that means individuals won't have access to alternatives.

Mike Godwin, *A Chip over My Shoulder: The Problems with Clipper*, INTERNET WORLD, July/Aug. 1994, at 92, 93.

[254] This is true even with the last alternative, because one can assume that the government would set the key length in accordance with what the NSA believes it could crack reasonably quickly.

2. *"Significant Governmental Interest"*

As with any content-neutral regulation, two competing interests are balanced: the extent to which communicative activity is inhibited, and the values, interests, or rights that will be served by enforcing the regulation.[255] Not only must a time, place, or manner regulation be narrowly tailored, it must also serve a significant governmental interest.[256] Some commentators equate "significant interest" with "important" or "substantial interest," which is lower than the "compelling interest" that the government must show to justify a content-based regulation.[257]

The government's rationale for a mandatory encryption scheme would be the same as was proposed for the adoption of EES.[258] Its concern is, once again, law enforcement's ability to understand what has been intercepted by a wiretap, and the NSA's ability to conduct signals intelligence. On the surface, the issue seems moot: after all, if the Court considers "ensuring the sufficiency of sound amplification at bandshell events" to be substantial,[259] surely wiretapping and signals intelligence would count as substantial. Other governmental interests that the Court has found substantial in upholding regulations include maintaining the condition of public parks,[260] avoiding distractions to traffic and protecting the quiet and tranquility of a municipality,[261] and preventing visual blight.[262] Although these seem relatively minor in comparison to the potential harm imposed by unfettered encryption, in those cases the "harm" *actually existed.* The government's rationales for mandatory encryption are serious, but at this point merely speculative.

The ability to wiretap is important to law enforcement, but encryption does not prevent wiretapping; it only makes the intercepted communication unintelligible. The government advocated EES in combination with its Digital Telephony Bill, which sought to have telephone companies modify their systems in order to make wiretapping easier.[263] The Telephony Bill, however, was a response to improved communications technology that actually

---

[255] TRIBE, *supra* note 208, § 12-23, at 979.

[256] Clark v. Community for Creative Non-Violence, 468 U.S. 288, 293 (1984).

[257] SMOLLA, *supra* note 173, § 3.02[3][A].

[258] *See supra* part I.D.

[259] Ward v. Rock Against Racism, 491 U.S. 781, 796-97 (1989).

[260] *Clark*, 468 U.S. at 288 (banning sleeping in public parks as a means to draw attention to plight of the homeless).

[261] Kovacs v. Cooper, 336 U.S. 77 (1949) (banning vehicle amplification devices that emit loud and raucous noises).

[262] Members of the City Council v. Taxpayers for Vincent, 466 U.S. 789 (1984) (upholding ban against posting signs on utility poles).

[263] *See supra* note 57.

prevented agencies from being able to adequately wiretap phone lines.[264] To date, there has been no harm to wiretapping from encryption: "the FBI has not been able to point to a single case to date where encryption has hampered their investigation of a case."[265]

Furthermore, serious questions have arisen as to the feasibility of wiretapping.[266] As James Kallstrom stated before the House Subcommittee, only 919 criminal wiretaps were authorized in 1992.[267] In 1993, 976 wiretaps were authorized, seventeen of which were never installed.[268] By way of comparison, in 1991 there were "approximately one-half trillion phone calls and over 140 million installed phone lines."[269] Thus, the percentage of wiretapped calls in relation to the total number of calls placed is very small.[270] Furthermore, only a few thousand people are arrested each year after wiretap investigations,[271] compared to 14 million overall arrests in 1991.[272] Of the 976 wiretaps authorized in 1993, seventy-three percent were in three states: New York, New Jersey, and Florida.[273] Also in 1993, nine states forbade the police to use wiretaps, and twenty-nine other states did not use them.[274] Finally, roughly seventy percent of wiretaps are used for narcotics offenses, and ten percent for gambling investigations.[275] These are the so-called "victimless crimes" and not the ones the law enforcement agencies usually tout as their justification for needing wiretaps. The FBI usually justifies the need for controlling encryption by arguing that encryption could render authorities unable to solve or prevent such heinous crimes as murder or kidnapping.[276] This could be a powerfully persuasive argument to the public, even more so now that such threats no longer seem

---

[264] Because of the digitalization of information, law enforcement agencies are not always able to intercept a complete conversation. *See* discussion *supra* notes 57-58 and accompanying text.

[265] Hoffman et al., *supra* note 34, at 115.

[266] Robin Hanson, *Can Wiretaps Remain Cost-Effective?*, COMM. ACM, Dec. 1994, at 13.

[267] *Hearing*, *supra* note 34, at 16 (statement of James K. Kallstrom, Deputy Director of the U.S. Department of Commerce, National Institute of Standards and Technology).

[268] Hanson, *supra* note 266, at 14.

[269] Banisar, *supra* note 32, at 501.

[270] *Id.*

[271] One statistical analysis puts the number of *convictions* at 7324 from 1985 to 1991. Hanson, *supra* note 266, at 14. These numbers do not reflect monetary fines and prevented economic loss.

[272] Banisar, *supra* note 32, at 501.

[273] Hanson, *supra* note 266, at 15.

[274] *Id.*

[275] *Id.* at 14. The actual percentage of wiretaps used for narcotics offenses in 1992 was 69%.

[276] Banisar, *supra* note 32, at 501; *see also* discussion *supra* notes 59-60 and accompanying text.

so far away. Using the threat of terrorism as justification, many Americans cannot help but recall the devastating images of the World Trade Center bombing and the bombing of the federal building in Oklahoma City. In reality, these types of crimes are rarely solved by wiretapping. In 1992, wiretaps were used three times in kidnapping investigations, and thirty-five times in murder investigations.[277] Moreover, some argue that wiretaps rarely *prevent* crimes, but are instead most often used *after* the crime has already been committed, to gather evidence about suspects.[278] Therefore, although wiretapping may assist law enforcement agencies in some investigations, the emergency situation the FBI and other law enforcement agencies cite is a very rare occurrence.[279]

Wiretapping may or may not be useful or feasible on a widespread scale. Nevertheless, because wiretapping's usefulness or feasibility is questionable—coupled with the fact that no harm has occurred to wiretapping from encryption—makes the government's case for mandatory encryption unconvincing. The feasibility of a wiretap also depends on the need for evidence, and whether it could be obtained by other means. Even in emergency situations, government agents will find out when they intercept the communication that it is encrypted. The need for real time decryption may be very great, but it is unclear whether any safeguards the government may institute, as was done with EES,[280] will allow for decryption in time to actually prevent a crime. The other, broader philosophical argument is that law enforcement officials should not be treating wiretapping as an "entitlement," and that privacy is too important to be set aside "just in case."[281] There may be an attitude on the part of law enforcement that they have a "right" to wiretap, and that technology should be accessible to them if and when the need to wiretap arises. As others have argued, government may conduct reasonable searches, but it is not entitled to an *effective* search.[282]

Due to the secrecy of the NSA's operations, fully evaluating their concerns for national security is difficult; however, the national security threat can be examined on a broader policy level. First, while the NSA is concerned about conducting signals intelligence within foreign nations, a mandatory encryption scheme is domestic in nature. The type and strength of encryption used by the rest of the world cannot be directly controlled by the United States. The NSA was prominent in the development of cryptography, and the United States as a whole is a leader in the field. Accordingly, the NSA understandably wants to use export controls to keep that technology

---

[277] Banisar, *supra* note 32, at 501.

[278] Godwin, *supra* note 253, at 94.

[279] *Id.*

[280] *See supra* notes 86-87 and accompanying text.

[281] Brody, *supra* note 10, at 27.

[282] *See* Froomkin, *supra* note 153, at 826-27.

from spreading outside U.S. borders. The fact remains, however, that DES-based products are *already* available worldwide, as are PGP, RSA, and 150 or so other products with DES-strength encryption.[283] To use a well-worn phrase, it looks as though the genie is out of the bottle.

Once the government's interests are examined, it is not easy to classify those interests as significant. So far encryption has done no harm domestically, and the United States is unable to control what happens outside its borders. Thus, the threat may not be as great as it seems, either because the technology will not be misused on the scale feared, or because the technology will not be used at all. For example, technology may have been successful in thwarting some terrorists, but

> [t]he danger for counterterrorists is in thinking that an array of fancy surveillance gear provides all the answers. Terrorists have found an easy and cheap way to evade the cops: go low-tech—or no-tech. They communicate not over the Internet but face to face; for destruction, they use a detonator that has so far proven unstoppable—a bomb-laden zealot.[284]

The government does not necessarily have to wait until disaster strikes, but it is important to weigh the interests of users against speculative harm, and not to overregulate blindly.

3. *"Open Ample Alternatives for Communication"*

The third prong of the Court's test provides the other side of the balance: whether the regulation leaves open ample alternatives for communication.[285] The crucial question will be deciding precisely what is considered an "alternative" to encrypted communications: some other means of confidential communications or non-encrypted communications.

The ability to communicate in confidence will be severely curtailed, if not lost altogether, if the government mandates either a particular encryption method or only key escrow. Arguably, one could find alternative private channels of communication in the form of face-to-face contact or in letter

---

[283] *See supra* notes 51-55 and accompanying text.

[284] Tom Masland et al., *Terrorism: A Battle on High—And Low*, NEWSWEEK, Feb. 27, 1995, at 40, 40.

[285] Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 771 (1976) (holding unconstitutional a statute prohibiting advertisements of prescription drug prices); *see* TRIBE, *supra* note 208, § 12-23, at 978-79.

writing.[286] The same argument was proposed against the Digital Telephony Bill:

> Telegrams, letters, or personal contact seem to be the main communication alternatives available to ensure similar confidentiality. Requiring personal contact, however, discriminates against those who cannot afford to travel, and neither telegrams nor letters provide instantaneous communication like telephone calls or e-mail.[287]

Although these methods may be private, they do not have the speed, versatility, or the ability to go beyond physical boundaries that electronic communications can offer. Comparing the advantages that electronic communications present, it is difficult to imagine that either clandestine face-to-face contact or the Postal Service qualify as true "alternatives" to encrypted communications.

Many cases have gone before the Supreme Court when a certain means of communication has been foreclosed.[288] Means of communication that have been previously targeted include leafletting,[289] door-to-door solicitation,[290] public solicitation,[291] sound trucks,[292] live entertainment,[293] street demonstrations,[294] billboards,[295] and signs on public utility poles.[296] These types of prohibitions have been found constitutional because the speaker has an alternative means of expression available.[297] The rationale behind the discussions is that elimination of any particular means of expression probably does not significantly reduce the total quantity of, and opportunities for, free expression.[298] Nevertheless, "[a]lthough prohibitions foreclosing entire media may be completely free of content or view-

---

[286] Metromedia, Inc. v. City of San Diego, 453 U.S. 490, 516 (1981); *see, e.g.*, Scheurer, *supra* note 153, at 284 (noting that "it may be argued that alternative channels for transmitting highly confidential information are available through the use of the mail").

[287] Nelson, *supra* note 57, at 1164.

[288] *See* Stone, *supra* note 210, at 64-67. The following cases are what he described as "the prohibited media cases." *Id.* at 64.

[289] Schneider v. State, 308 U.S. 147 (1939).

[290] Martin v. Struthers, 319 U.S. 141 (1943).

[291] Schaumburg v. Citizens for a Better Env't, 444 U.S. 620 (1980).

[292] Kovacs v. Cooper, 336 U.S. 77 (1949).

[293] Schad v. Mount Ephraim, 452 U.S. 61 (1981).

[294] Cox v. Louisiana, 379 U.S. 536 (1965).

[295] Metromedia, Inc. v. City of San Diego, 453 U.S. 490 (1981).

[296] Members of the City Council v. Taxpayers for Vincent, 466 U.S. 789 (1984).

[297] Stone, *supra* note 210, at 64-65.

[298] *Id.*

point discrimination, the danger they pose to the freedom of speech is readily apparent—by eliminating a common means of speaking, such measures can suppress too much speech."[299]

According to Tribe, one factor that weighs in the balance is the degree to which such a regulation "falls unevenly upon various groups in the society."[300] This factor arguably played a large role in the Court's decision in *City of Ladue v. Gilleo*,[301] in which the Court struck down a ban on residential signs, noting that they are "an unusually cheap and convenient form of communication. Especially for persons of modest means or limited mobility, a yard or window sign may have no practical substitute."[302] In analyzing a mandatory key escrow scheme, Professor Froomkin argues that the impact would fall unevenly on those with access to such devices—a group that differs greatly from those the Court traditionally protects the most: the poor and those that are without access to alternative means of communication.[303] Given the growth of electronic communications over the past several years, and the fact that forecasters predict that almost everything will be done electronically—including banking and shopping—such a regulation potentially impacts a majority of the population of the United States. The key to deciding the weight of the government's interest in restricting encryption will be the importance with which a court views the confidentiality of the message to be, and whether encryption would inhibit free expression.[304]

In addition to personal contact and regular mail, another alternative to encrypted communications is the use of non-encrypted communications.[305] The benefits of electronic communications—speed and the number of potential listeners—remain intact, and mandatory encryption still provides some security. Requiring keys to be escrowed or using only government-approved encryption means that the communication would not be completely confidential, and thus may not be a "true" alternative to communications encrypted by the user's choice of method. Many encryption methods can arguably be deciphered by the cryptography experts at NSA, but there is a significant difference to the user between someone "cracking" their encryption code and handing over the keys ahead of time. The argument that some security

---

[299] City of Ladue v. Gilleo, 114 S. Ct. 2038, 2045 (1994).

[300] TRIBE, *supra* note 208, § 12-23, at 979.

[301] 114 S. Ct. 2038 (1994).

[302] *Id.* at 2046.

[303] Froomkin, *supra* note 153, at 816.

[304] Froomkin finds that this inhibition would be fairly minor, given that the keys would only be released for just cause. *Id.* at 816-17. For a more detailed evaluation of the possible chilling effect of mandatory encryption, see discussion *infra* part III.B.5.

[305] The term "non-encrypted communications" refers to electronic communications that cannot be encrypted with the user's choice of encryption method, as would result under a mandatory encryption scheme.

insured by the government is better than no security minimizes both the importance of having a completely confidential means of communication and the chilling effect on speech that may occur if there is no longer such privacy.

5. *Possible Chilling Effect of Mandatory Encryption*

a. *Traditional Chilling Effect Analysis*

Beyond the doctrinal examination into the implications of mandatory encryption, there lurks a broader, more philosophical inquiry as to the effects of such a policy on free speech. With no empirical studies to analyze, the question of whether the absence of a completely confidential means of communication will "chill" speech is purely hypothetical.[306] Although no definitive answer can be given, after examining the traditional arguments for finding a chilling effect, this section will outline the factors that must be taken into account before deciding whether a mandatory encryption scheme would chill speech—and perhaps before the entire constitutionality question may be answered.

A "chilling effect" occurs when people are deterred from participating in a particular activity.[307] In the area of First Amendment free speech, the notion of a chilling effect takes on a more sinister tone—self-censorship—as people are deterred from expressing themselves as they otherwise might.[308] This self-censorship arises out of fear of punishment—a fear that arises because the legal process is riddled with uncertainty, and individuals are afraid that what they may say is too close to the line.[309] Tribe explains this phenomenon in the context of defamation law as "a great danger . . . aris[ing] from the fear of guessing wrong—the fear that the trier of fact,

---

[306] Professor Froomkin has advocated that speech would be chilled by a mandatory encryption scheme, but admits that it would be difficult to collect evidence on the subject. Froomkin, *supra* note 153, at 815-16 & n.452.

[307] Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect"*, 58 B.U. L. REV. 685, 689 (1978).

[308] *Id.* at 690-92. This is to be contrasted with the general notion of a chilling effect as a deterrent, which has neither a negative nor a positive connotation, as many laws, especially criminal laws, are specifically designed to proscribe—"chill"—certain undesirable activity. *See id.* at 689-90. In the First Amendment context, Schauer defines chilling effect as occurring "when individuals seeking to engage in activity protected by the [F]irst [A]mendment are deterred from so doing by governmental regulation not specifically directed at that protected activity." *Id.* at 693.

[309] *See id.* at 694-701. As the Supreme Court has noted, "where particular speech falls close to the line separating the lawful and the unlawful, the possibility of mistaken factfinding—inherent in all litigation—will create the danger that the legitimate utterance will be penalized." Speiser v. Randall, 357 U.S. 513, 526 (1958).

proceeding by formal processes of proof and refutation, will after the event reject the individual's judgment of truth."[310]

As a result of this uncertainty, individuals "restrict[] their conduct to that which is unquestionably safe."[311] Such self-censorship does not occur only after being charged, for "[t]he *threat* of sanctions may deter [the exercise of First Amendment freedoms] almost as potently as the actual application of sanctions."[312] Furthermore, the likely outcome of any prosecution does not necessarily relieve the speaker. "The chilling effect upon the exercise of First Amendment rights may derive from the *fact* of the prosecution, unaffected by the prospects of its success or failure."[313] Self-censorship is especially common where the individual, rather than the government, would bear the burden of proof at trial, for "[t]he man who knows that he must bring forth proof and persuade another of the lawfulness of his conduct necessarily must steer far wider of the unlawful zone than if the State must bear these burdens."[314]

The consequence of self-censorship is that freedom of speech is not fully exercised and society ultimately bears the loss.[315] "The danger of this sort of invidious chilling effect lies in the fact that something that 'ought' to be expressed is not. Deterred by the fear of punishment, some individuals refrain from saying or publishing that which they lawfully could, and indeed, should."[316] Simply put, where the line is gray—as much of the First Amendment is—individuals may not expend the time and energy to calculate where exactly the line is; instead they will either restrict their speech to that which is safe, or say nothing at all.

The application of the chilling effect doctrine is most readily seen in cases which define the line between protected and unprotected speech: defamation,[317] obscenity,[318] and incitement or advocacy of imminent lawless-

---

[310] TRIBE, *supra* note 208, § 12-12, at 863-64.

[311] Baggett v. Bullitt, 377 U.S. 360, 372 (1964).

[312] NAACP v. Button, 371 U.S. 415, 433 (1961) (emphasis added).

[313] Dombrowski v. Pfister, 380 U.S. 479, 487 (1965) (emphasis added).

[314] Speiser v. Randall, 357 U.S. 513, 526 (1958).

[315] Schauer, *supra* note 307, at 693.

[316] *Id.*

[317] *See, e.g.*, New York Times v. Sullivan, 376 U.S. 254, 279-80 (1964) (prohibiting "a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice'—that is, with knowledge that it was false or with reckless disregard of whether it was false or not"); *see also* Schauer, *supra* note 307, at 705-14.

[318] *See, e.g.*, Miller v. California, 413 U.S. 15, 24 (1973) (setting the basic guidelines for defining obscenity as "(a) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest . . . ; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political or scientific value"); *see*

ness.[319] With each example, the Court has struggled to define exactly what kind of speech falls into each category, in an effort to provide some guidance as to what is constitutionally protected speech, and arguably to reduce any chilling effect. Apart from content categories of speech, particular regulations which allegedly chill speech can be challenged on either overbreadth[320] or vagueness[321] grounds. According to Tribe, both of these doctrines represent the notion that "in close cases, government must leave speech ample room to breathe."[322] Frederick Schauer goes a step further, advocating that the First Amendment is the preferred value, and therefore, realizing that errors will be made in the judicial process, the chilling effect doctrine states that rules and procedures should be designed to err on the side of free speech.[323]

b. *Factors in Deciding Whether Mandatory Encryption Would Chill Speech*

The foregoing analysis presupposes that we are dealing with a problem of defining whether speech is in a protected or unprotected category, or that a specific regulation affecting the exercise of free speech is at issue. Analyzing the possible chilling effect caused by a mandatory encryption scheme does not fit into either "traditional" usage of the argument. Instead, we are

---

also Schauer, *supra* note 307, at 714-21.

[319] *See, e.g.*, Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (holding that the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action); *see also* Schauer, *supra* note 307, at 721-25.

[320] A law is overbroad if "it 'does not aim specifically at evils within the allowable area of [government] control, but . . . sweeps within its ambit other activities that constitute an exercise' of protected expressive or associational rights." TRIBE, *supra* note 208, § 12-27, at 1022 (alteration in original) (quoting Thornhill v. Alabama, 310 U.S. 88, 97 (1940)). The danger lies in the fact that "an 'overbroad' law . . . 'hangs over [people's] heads like a Sword of Damocles.' That judges will ultimately rescue those whose conduct in retrospect is held protected is not enough, 'for the value of a Sword of Damocles is that it hangs—not that it drops.'" TRIBE, *supra* note 208, § 12-27, at 1023 (citation omitted) (quoting Arnett v. Kennedy, 416 U.S. 134, 231 (1974) (Marshall, J., dissenting)).

[321] Tribe explains that:

> [a]s a matter of due process, a law is void on its face if it so vague that persons "of common intelligence must necessarily guess at its meaning and differ as to its application." Such vagueness occurs when a legislature states its proscriptions in terms so indefinite that the line between innocent and condemned conduct becomes a matter of guesswork.

Id. § 12-31, at 1033 (citation omitted) (quoting Connally v. General Constr. Co., 269 U.S. 385, 391 (1926)).

[322] *Id.* § 12-33, at 1039.

[323] Schauer, *supra* note 307, at 732.

left with a much broader philosophical inquiry—would speech be chilled due to the lack of confidentiality of electronic communications? Stated differently, would knowing that the government had the means to decrypt their electronic communications cause individuals to refrain from using the medium; alternatively, would they be deterred from speaking freely, from debating or criticizing policies or positions, or from advocating unpopular opinions?

This question can only be answered on an individual level, and only after considering a number of factors. Yet this imprecision is not a fatal flaw in chilling effect analysis, for admittedly *all* chilling arguments are based on what the likely effect would be on individuals, without conclusive, or perhaps any, proof of that effect. As Schauer states:

> While the chilling effect concept appears to be premised on predictions or assumptions about human behavior, no evidence has been proffered to justify those predictions. It has not been clearly established that individuals are mistakenly deterred or become overly cautious as a result of the existence of particular statutes, rules or regulations. Yet it surely is not to be expected that courts will always abstain from making or accepting assumptions about human behavior; behavior is, after all, that with which the law is fundamentally concerned.[324]

Although there is no definitive way to tell whether speech would be chilled, this Note will identify certain factors which should be considered in weighing any possible chilling effect.

The first factor to be examined is the exact scope of authority that the government would have in obtaining cryptographic keys. If no safeguard is provided, and the government is allowed to freely monitor transmissions, then a chilling effect argument seems very viable. In fact, it is difficult to imagine that there would *not* be a chilling effect, given basic knowledge about human behavior—that individuals behave differently when they believe they are being observed.[325] Some common examples include the rush to "look busy" when a supervisor enters the office or work area; the difference between what we discuss with others as opposed to what we write in

---

[324] *Id.* at 730.

[325] A current example of this phenomenon is the seemingly exponential increase in the number of video cameras around us. The fear is that "as security cameras and amateur camcorders multiply around us, our zone of privacy shrinks. All those lenses aimed at us inflict a chilling effect on everyday behavior." Bill Stamets, *Camcorders: When Is Recording a Protected Right, and When Is It an Invasion of Privacy?*, CHI. SUN-TIMES, Mar. 4, 1994, at 54.

diaries; and the difference in tone and content of a telephone conversation when one is calling from a private office as opposed to a crowded room. A mandatory encryption scheme is unlikely to give the government blanket authority to monitor electronic transmissions. Instead, government agents probably would be required to obtain a search warrant before they could obtain any keys. The question remains whether a warrant-type safeguard would result in complete "confidentiality" in the users' minds, and whether it would chill speech.

These questions ultimately relate to the *perception of confidentiality* under a mandatory encryption scheme. A comparison to other technologies illustrates the connection. For example, both cellular and cordless phones are notorious for their lack of security. Cellular phones are vulnerable to eavesdropping through radio scanners, and illegal use of their networks costs cellular carriers an estimated $500 million per year.[326] Similarly, cordless phone transmissions are easily intercepted by other cordless phones, radio scanners, and even baby monitors.[327] In fact, cordless phone customers are often advised to not say anything that "they wouldn't want to see on the front page of their local newspaper."[328] Although technology is improving, persuasive proof of cordless phones' reputation for vulnerability may be found in federal court decisions. Until recently, these decisions held that cordless phone users retained *no expectation of privacy* under the Fourth Amendment.[329] It is a logical conclusion that as a result of such decisions, people are now more careful about what they say over these phones.[330]

E-mail has also received a fair amount of publicity for its general lack of security. The outcry for security measures, including the Clipper Chip controversy,[331] is evidence that confidentiality is among the top concerns of electronic communications users. This concern may indicate either a perception that inadequate confidentiality will chill speech, or it may simply

---

[326] Chris O'Malley, *The Wireless World: The Information Skyway Is Coming Soon to a Wireless Device Near You*, POPULAR SCI., Nov. 1995, at 56, 56.

[327] *Cordless Phones (Buyers Guide)*, GOOD HOUSEKEEPING, Aug. 1995, at 38, 38.

[328] Alexandra Alger, *For Your Ears Only (Digital Cordless Phones)*, FORBES, Oct. 23, 1995, at 358.

[329] *See* United States v. Smith, 978 F.2d 171, 176-81 (1992); Junda Woo & Jonathon M. Moses, *Cordless-Phone Users Win Degree of Protection From Eavesdroppers*, WALL ST. J., Nov. 17, 1992, at B16.

[330] Nevertheless, there are exceptions to this "common sense" argument. A Memphis couple was charged with conspiracy to murder the woman's husband, after their cordless phone conversation was picked up by a police scanner of a another Memphis resident—who was able to identify the female conspirator as the mother of one of her daughter's friends. *See* Margo Kaufman, *What Eavesdroppers Know (and You Should Learn)*, REDBOOK, May 1995, at 62, 63.

[331] *See* discussion *supra* part II.B.

be a backlash against the government's perceived attempt to force users to relinquish their preferred security measures. The latter interpretation may be reinforced by the fact that electronic communications users have more control over keeping their communications confidential, whereas telephone users are virtually powerless.[332] In other words, the protests are a result of the users not wanting to lose the control they already have, not because they are afraid of what the government may hear.

As a psychological matter, users' perception of confidentiality strongly influences how freely they speak through electronic communications. Clear safeguards will also increase the chances of a successful mandatory encryption scheme. The government would be perceived as minimizing intrusions on liberty, and users' fears would look more irrational. The greatest chill on telephone conversations, for example, seems to result from the lack of physical, rather than technological, privacy. On balance, people will probably feel a similar chill with electronic communications as they do with the telephone—assuming it is not a cordless or cellular phone. Nevertheless, additional security concerns surround electronic communications. For example, unlike telephone conversations, e-mail can be searched for particular words or phrases, and a transmission can be downloaded and saved for some future use. Electronic communications, however, also add an element of anonymity that is lacking in telephone communications. Technologically, it is possible to transmit completely anonymous electronic messages.[333] Psychologically, one does not have to reveal their name or address to communicate electronically, and communication can take place in a completely private setting—such as one's personal computer at home. Moreover, perception of confidentiality is often colored by the level of trust placed in the government. As previously noted, few trust the government with the task of keeping the keys confidential.[334]

The probability of a chilling effect and the perception of confidentiality also depend on other factors, including the identity or sophistication of the speaker and the subject matter discussed. The identity or sophistication of the user plays a major role, in that those who are unaware of security risks, and whose primary use is e-mail as a substitution for regular mail, will not likely have their speech chilled by a mandatory encryption scheme. On the other hand, a more sophisticated user of electronic communications, who participates vigorously in public debate and discussion of unpopular ideas,

---

[332] This is not to say that there are no security measures available for consumers with respect to telephones, but in general, such measures require buying a telephone with the security device already hardwired in it. This is not only expensive, but it can also lead to problems finding someone else with a telephone that can "decode" the conversation.

[333] "Completely anonymous" messages refers to the ability to send messages over computer networks in such a manner that the transmission cannot be traced back to its point of origin or its author.

[334] *See supra* note 116 and accompanying text.

will more likely be affected. Similarly, the advent of computer networks has opened a wide forum for debate and arguably has drawn out more people—those who may not be comfortable speaking out in a crowd. Thus, reaction to a mandatory encryption scheme will vary with the speaker, but because our society values all types of expression, the chilling effect argument is not lessened.

The next factor in determining the chilling effect of mandatory encryption is the subject matter carried by electronic communications. For example, users who are merely substituting e-mail for regular mail probably will not be concerned with a mandatory encryption scheme. For those engaging in business, or who are heavily involved in public policy debate or opposition groups, the ability to speak freely often depends on perceived confidentiality and consequences of monitoring. A lack of confidentiality and the ability to monitor freely would almost certainly chill business-related speech, for even though a mandatory encryption scheme would arguably be content-neutral,[335] all of the uncertainties inherent in First Amendment jurisprudence are present.

No hard scientific data defines the point at which people will engage in self-censorship. Although the preceding factors describe perceptions and emotions, they are illustrative because chilled speech results from fear and uncertainty of the reaction to such speech. As Schauer notes: "the chilling effect doctrine flows not from a *specific behavioral state* of the world, but from an understanding of the comparative nature of the errors that are bound to occur."[336] Obviously, the more irrational the fear, the less likely a chilling effect argument will be successful. Nevertheless, the foregoing factors should be weighed before the constitutionality of mandatory encryption is decided. Absent a substantial governmental interest that can be safeguarded only by restricting free speech, "[b]ehavioral ignorance or imprecision must be resolved in favor of excess permission, not over-restriction."[337]

CONCLUSION

Just as Pool predicted—as the floodgates of private discourse continue to open wider in cyberspace, the government is attempting to shut the gates by controlling encryption. From the government's perspective, the only way to alleviate the risks underlying completely confidential communications is through a mandatory encryption scheme. When applying traditional First Amendment principles, such a scheme looks inherently like a content-neutral time, place, or manner regulation. Courts will have to balance the

---

[335] *See* discussion *supra* notes 229-32 and accompanying text.

[336] Schauer, *supra* note 307, at 731 (emphasis added).

[337] *Id.*

government's interest in eliminating threats to law enforcement and national security against the right to, and need for, a completely private means of communication, along with any chilling of speech that may occur without confidentiality guarantees.

Electronic communications as a whole, and encryption in particular, admittedly do not fit perfectly within the traditional First Amendment framework. The government's harms, though speculative now, are serious and very much within the realm of possibility. In the long run, it is unimportant that the First Amendment fit is less than perfect, or that the specified harm has not come to pass. Rather, it is important to recognize that the First Amendment's free speech principles are applicable, and ensure that individual rights are fully, objectively, and rationally considered, and not silenced solely out of fear or overreaction.

JILL M. RYAN