University of Dayton Law Review

Volume 23
Number 1 *Joseph E. Keller Hall Dedication Issue*

Article 6

10-1-1997

Escrowed Encryption Systems: Current Public Policy May Destroy Valued Constitutional Protections

Wyman P. Berryessa
University of Dayton

COMMENTS

ESCROWED ENCRYPTION SYSTEMS: CURRENT PUBLIC POLICY MAY DESTROY VALUED CONSTITUTIONAL PROTECTIONS

Wyman P. Berryessa[*]

TABLE OF CONTENTS

---

[*] Executive Editor, University of Dayton Law Review. J.D., 1998, University of Dayton School of Law; B.B.A., 1994, University of Middle Tennessee.

I. INTRODUCTION

> In the walls of the cubicle there were three orifices. To the right of the speakwrite, a small pneumatic tube for written messages; to the left, a larger one for newspapers; and in the side wall, within easy reach of Winston's arm, a large oblong slit protected by a wire grating. This last was for the disposal of waste paper. Similar slits existed in thousands or tens of thousands throughout the building, not only in every room but at short intervals in every corridor. For some reason they were nicknamed memory holes.[1]

Samuel Johnson stated, "to keep your secret is wisdom; but to expect others to keep it is folly."[2] The Clinton Administration's current policy concerning encryption technology is asking the American public to commit this folly. The purpose of the policy is to encourage the American public to voluntarily opt into an escrowed encryption system (EES) which would give the government access to all electronic communications within the system.[3] The justification for promoting an EES is to maintain the government's ability to conduct successful wiretapping of suspected criminal communications.[4]

Once described as a niche market,[5] encryption technology is becoming a prevalent necessity of American industry.[6] Furthermore, private individuals are utilizing encryption technology to keep their private communications confidential. Although the public has traditionally been skeptical of keeping information confidential on the Internet, encryption technology promises to achieve this goal.[7] Present encryption technology can keep private communications from observation of third parties, and in conjunction with digital signatures, can confirm the authenticity of those communications.[8] The importance of encryption technology is that its potential use promises to make the Internet a valuable tool for commerce

---

[1] GEORGE ORWELL, 1984 34-35 (1949) (describing the "Ministry of Truth").

[2] DONALD O. BOLANDER ET AL., INSTANT QUOTATION DICTIONARY 234 (1969) (quoting Samuel Johnson).

[3] 141 CONG. REC. E2307 (1995) (statement of Rep. Bob Goodlatte).

[4] A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 715 (1994).

[5] SUSAN LANDAU ET AL., ASSOCIATION FOR COMPUTING MACHINERY, INC., CODES, KEYS, AND CONFLICTS: ISSUES IN U.S. CRYPTO POLICY 12 (1994).

[6] 142 CONG. REC. S1516 (1996) (statement of Sen. Leahy).

[7] BRUCE A. LEHMAN, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 183-88 (1995).

[8] *Id.* at 185-88.

and a powerful medium for communicating personal information.[9] However, this emerging possibility is being tempered by the fear of criminal secrecy, and the government is using this concern as a mantra for ensuring that it has access to every electronic communication that occurs in the United States.[10]

The current policy of the Clinton Administration promotes the assurance, through governmental manipulation of the market, that the government will be able to gain access to every electronic communication via an escrow agent who holds the "key" to all encrypted communications within the system.[11] This governmental policy is known as a voluntary escrowed encryption system. This policy has been formed in the wake of public rejection of a mandatory escrowed system.[12] A mandatory system has been rejected in the midst of fear of First Amendment, Fourth Amendment, Right to Privacy, and other potential constitutional violations.[13] However, the voluntary EES and mandatory EES policies both rest on the governmental interest of maintaining its ability to continue surveillance of electronic criminal communications. As this Comment will address, the voluntary policy may be the government's attempt to establish the prevalence of an EES. Thereafter, the government will have arguable grounds for implementing a mandatory EES policy. In the end, the potential constitutional infringements may be identical. Facilitating the Government's ability to implement mandatory EES is not only a bad policy choice, it is contradictory to our republican form of government. Whereas the United States' form of government is based on the principle that "[G]overnments are instituted among Men, deriving their just powers from the consent of the governed,"[14] those "who trust secrets to a servant makes him his master."[15] This Comment is sensitive to the fact that the government may lose a valuable investigatory tool because of strong encryption technology, but underlying its concerns is the belief that "too

---

[9] FDCH POLITICAL TRANSCRIPTS, UNITED STATES DEPARTMENT OF COMMERCE HOLDS HEARING ON COMPUTER SECURITY AND ENCRYPTION (comments of Mr. Geer) (Federal Document Clearing House, Inc., Nov. 26, 1996) [hereinafter *FDCH*].

[10] 142 CONG. REC. S1516 (1996).

[11] *See infra* notes 90-94 and accompanying text.

[12] In such a mandatory system, it would be illegal to use any encryption technology except that form chosen by the government. Philip Elmer-Dewitt, *Who Should Keep the Keys?*, TIME, Mar. 14, 1994, at 90.

[13] *See* discussion *infra* part III.B.

[14] THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776).

[15] BOLANDER, *supra* note 2, at 234 (quoting John Dryden).

many people are thinking of security instead of opportunity. They seem more afraid of life than death."[16]

The purpose of this Comment is to expose the potential results of acceptance and compliance with a voluntary EES policy. The potential result is that the government may undermine major portions of the Bill of Rights by adopting a mandatory EES policy after compliance with a voluntary EES policy establishes the prevalence of that system.[17] Furthermore, this Comment highlights the fact that industry and the American public presently have the choice not to opt into this or any other governmentally accessible system. Section II of this Comment details the nature and evolution of encryption technology.[18] Section III of this Comment discusses the respective considerations of adopting a voluntary or mandatory EES policy.[19] This Section argues that the potential prevalence of a voluntary escrowed encryption system will allow the government to constitutionally mandate an escrowed encryption system in the future because its prevalence would alter the constitutional analysis which presently seems to prohibit the government from mandating an escrowed encryption system.[20] Section IV of this Comment concludes that encryption technology will most likely play a significant role in the future of America, and before the public complies with any voluntary escrowed encryption system, the public needs to consider whether it is worth losing constitutional protections in order to allow the government to monitor electronic communications.

II. BACKGROUND

In order to understand the current voluntary escrowed encryption system policy, it is first necessary to understand the nature of encryption technology. Furthermore, it will be helpful to understand the evolution of encryption technology and the respective regulations that have coincided with the advent of more sophisticated capabilities. This Section will educate the reader and provide an adequate background to understand the justifications for accepting or abandoning President Clinton's or any other voluntary EES policy.

---

16 *Id.* (quoting James F. Byrnes).

17 *See infra* notes 105-160 and accompanying text.

18 *See infra* notes 21-75 and accompanying text.

19 *See* discussion *infra* part III. A-B.

20 *See infra* notes 76-160 and accompanying text.

A. The Nature of Encryption Technology

If one has ever utilized a decoder ring or used "pig-Latin" in elementary school, he is somewhat familiar with encryption technology. Encryption is merely some type of pre-established formula whereby any message can be disguised.[21] Its utility derives from the fact that only those who know the pre-established formula can decipher its meaning.[22] Its security derives from the ability of the sender and recipient to keep others from breaking the pre-established formula.[23] While substituting respective numbers for letters or moving the first consonant of a word to the end and adding "ay" may be simple formulas to break, current computer technology has developed many formulas that are practically impossible to break.[24] Not dissimilar from the elementary school bully, who became infuriated when one person spoke in cipher to another in front of him, the United States government is frustrated with the public's ability to communicate in secrecy.

Consistent with any form of cipher, modern computer encryption technology utilizes a formula that disguises whatever information to which it is applied.[25] The formula that it utilizes is called an algorithm.[26] Although effective algorithms are very sophisticated, they still perform the same purpose as a simple formula. That is, they take a message, apply it to a pre-established formula, and produce a facially meaningless message that can be deciphered only by those who also know the formula.[27] In fact, the only characteristic that technologically separates modern algorithms from simple formulas is the ability to utilize variations of the formula which are established upon each communication. This makes it possible for a third parties to know the algorithm and yet still not be able to understand any particular communication because they do not know what variant is being used.[28]

---

[21] DAVID KAHN, THE CODEBREAKERS xvi (1967).

[22] *Id.* at xv.

[23] Froomkin, *supra* note 4, at 713-14.

[24] *Id.* at 887-88.

[25] *See supra* note 21, at xvi.

[26] LEHMAN, *supra* note 7, at 186.

[27] Eric Bach et al., *Cryptography FAQ* at 3 (visited Oct. 31, 1994) <fttp://rftm.mit.edu/pub/usenet /news/answers/cryptograpgy-faq/part03>.

[28] Froomkin, *supra* note 4, at 754.

Modern computer encryption technology can, simplistically, be broken into two groups. The first group is a "single key" system.[29] The second group is a "public key" system.[30] A single key system is an encryption method where both the sender and recipient previously know what algorithm, or variant thereof, will be used.[31] A variant of any algorithm in this system is created by the use of a "session key."[32] A session key is a string of characters that is applied to an algorithm before a message is sent and must be known by both the sender and receiver.[33] The sender enters her communication, the algorithm disguises the message, the disguised message is sent through an electronic medium, the recipient receives and decrypts the message through the use of the same algorithm, and reads the original message as the sender has entered.[34] Once a link has been established between the two parties, they can each communicate back and forth in a rapid and secure manner.[35]

A public key system utilizes many of the same mechanisms of a single key system, however, it uses a "private key" and a "public key."[36] A private key is a string of characters which belongs to and is known only to the user.[37] A public key is a string of characters that belongs to the user but is made available to the public.[38] In effect, the user's public key is used to identify the user similar to a telephone number or street address. In order to send a disguised message in a public key system the sender and recipient must first be using equipment or software that utilizes the same algorithm. The sender then enters the plain text and disguises the message by applying it to a variant of the algorithm.[39] The variant is created by entering the desired recipient's public key.[40] Once encrypted in this fashion, the only person who can decrypt the message is one who has the private key which is correlated to the public key of the intended recipient.[41] Therefore, once the recipients receive the disguised message, they undisguise the message

---

29 *Id.* at 714.

30 *Id.*

31 LEHMAN, *supra* note 7, at 186.

32 Froomkin, *supra* note 4, at 892.

33 *Id.* at 890-91.

34 *Id.* at 891.

35 KAHN, *supra* note 21 at xv.

36 LEHMAN, *supra* note 7, at 186.

37 *Id.*

38 *Id.*

39 *Id.*

40 *Id.*

41 LEHMAN, *supra* note 7, at 186.

using a variant of the algorithm which is created by entering their private key.[42]

The utility of a single key system lies in its speed of communication and its secure nature.[43] The ability of this system to facilitate rapid communications is beyond the scope of this article,[44] but its security derives from the fact that only two parties need to know the algorithm that will be used. Simply speaking, as long as a sophisticated algorithm is used for one message, and as long as the parties do not reveal the algorithm to anyone else, the communication is nearly impossible to break in a timely manner.[45] The downside to this system, however, is that both parties must have previously known each other, established an algorithm to be used, and be able to trust each other not to divulge the algorithm to any other party.

On the other hand, a public key system allows unrelated parties to securely communicate without ever meeting or establishing a particular algorithm to be used for a communication session.[46] As long as two parties are using the same generic encryption algorithm and one has the public key of the other, a communication link can be established.[47] The ability for unrelated parties to send unsolicited messages to each other obviously makes this system superior for establishing a communication infrastructure.[48] Utilizing this system could eventually lead to a world where a public keys are listed next to telephone numbers in directories and secure commercial or personal communications could be sent. However, this system is predicated on the fact that everyone in the directory would be using software or hardware which utilizes the same generic algorithm.[49]

---

[42] Because modern technology only allows this type of system to communicate at slow speeds, users in these systems often wish to utilize the speed of a single key system. Froomkin, *supra* note 4, at 892. This is accomplished by having the sender relay an encrypted session key that will be used for the conversation. *Id.* After the recipient receives the desired session key from the sender, they apply it to the algorithm and a secure channel will result for the duration of the conversation. *Id.* Again, even if third parties were to know of the generic algorithm that the sender and receiver are using, they would be unable to decipher the contents of the communications during that session, unless they could figure out what session key was being used.

[43] *Id.* at 892.

[44] For a discussion of technical capabilities see Paul Fahn, RSA Laboratories, *Answers to Frequently Asked Questions About Today's Cryptography*, (last updated May 29, 1996) <fttp://rsa.com/rsa.com/rsa.labs/newfaq/q1.html>.

[45] Froomkin, *supra* note 4, at 887.

[46] LEHMAN, *supra* note 7, at 186.

[47] *Id.*

[48] A public key infrastructure's ability to facilitate unsolicited communications would allow such commercial necessities as sending offers, consumer purchases, or inter-company transmission of trade secrets.

[49] *See supra* notes 26-50 and accompanying text.

This creates the need for some form of standardization for an encryption system. For security purposes, this system raises the problem of who will create the private keys and how they will protect them.[50]

B. The Evolution of Encryption Technology and Its Regulation

The most prevalent utilization of encryption technology has historically rested in the hands of the government and the military.[51] Although various types of encryption technology have been used, the government adopted the Data Encryption Standard (DES) in the early 1970's.[52] DES has been used by the government for the transfer of non-classified information.[53] Other prominent users of encryption technology have been banks and other financial institutions.[54] These institutions use encryption technology to protect information regarding such uses as wire transfers and ATM transactions.[55] In addition to these prominent users, private individuals are also starting to frequently utilize encryption technology.[56] Private individuals use encryption for such purposes as faxing documents over the phone lines and sending e-mail to friends.[57] Unfortunately, private individuals also use encryption technology to disguise criminal communications.[58]

In response to commercial and private use of encryption technology, the government has attempted to implement several laws and regulations regarding its use. With the purpose of maintaining the government's ability to monitor encrypted communications, the government has made it illegal to export any encryption technology stronger than DES.[59] This type of encryption technology is treated as munition and can only be exported

---

[50] Froomkin, *supra* note 4, at 803 (arguing that entrusting a third party escrow agent with private keys raises additional security considerations).

[51] LANDAU, *supra* note 5, at 12; Richard L. Field, *Banking Has Important Stake in Unfolding Cryptography*, 16 No. 2 BANKING POL'Y REP. 5.

[52] Froomkin, *supra* note 4, at 735.

[53] Revision of Federal Information Processing Standard (FIPS) 46-1 Data Encryption Standard (DES), 58 Fed. Reg. 69,348 (1993).

[54] Ivars Peterson, *Encryption Controversy*, 143 SCI. NEWS 394, 395.

[55] Froomkin, *supra* note 4, at 719-20.

[56] Private use of encryption technology became somewhat popular through the advent of Pretty Good Privacy (PGP) software. *Id.* PGP, created by Phil Zimmerman, is military-grade encryption software and is freely available on the Internet. *Id.*

[57] Froomkin, *supra* note 4, at 729.

[58] *Id.*

[59] International Traffic in Arms Regulation (ITAR), 22 U.S.C. § 2778.

with prior permission from the government.[60] However, only financial institutions have historically been able to routinely get permission to use this strong type of encryption for international communications.[61] Until recently, the government had not attempted to proscribe domestic use of encryption technology, but with the advent of public key systems and broadening private use of encryption technology, the government has considered different policies to assure that it can access domestically encrypted communications.

The government's first major attempt to control the domestic use of encryption technology was through the advent of the Clipper Chip.[62] The Clipper Chip was electronic hardware that would be installed within a computer.[63] The device would facilitate the encryption of communications between computers using the Clipper Chip in a public key system.[64] The distinctive feature of the Clipper Chip is that it would allow the government to monitor communications within the system.[65] The monitoring mechanism is made possible through the use of the Law Enforcement Access Field (LEAF).[66] The LEAF would allow police officials to wiretap phone lines and receive serial numbers of individual Clipper Chips.[67] After receiving the serial number, the law enforcement officials would contact an escrow agent who would have the private key which correlated to that serial number.[68] After receiving the private key of the user, law enforcement officials would then be able to decrypt the encrypted messages that were being sent and received from that computer.[69] The escrow agent under the Clipper Chip public key system would have remained solely within the control of the government.[70]

The potential requirement of mandating the use of the Clipper Chip raised several heated debates.[71] The idea that the government may require a computer chip to be placed in everyone's computer enraged many civil

---

60 22 C.F.R. §§ 120-30 (1994).

61 Froomkin, *supra* note 4, at 737.

62 *See* Edmund L. Andrews, *Federal Agencies Get OK for High-Tech Wire Taps*, SAN FRAN. CHRON., Feb. 5, 1994.

63 Robert L. Hotz, *Demanding the Ability to Snoop*, L.A. TIMES, Oct. 3, 1993, at A1, A31.

64 *Id.*

65 *Id.*

66 Froomkin, *supra* note 4, at 755.

67 *Id.* at 755-57.

68 *Id.* at 757.

69 *Id.* at 758-59.

70 *Id.* at 752.

71 *See e.g.*, The Clipper Chip Debate, WL, US Testimony Database, 1994 WL 231119.

libertarians and invoked visions of "Big Brother."[72] Although law enforcement officials would be able to legally conduct wiretaps only with a search warrant, the fact remains that the government would be entrusted with the private keys to everyone's communications. This situation has been analogized to the public being forced to give the keys of its homes to the government just in case a search warrant is executed in the future.[73] Although the government has considered very confidential procedures for manufacturing and recording the respective serial numbers and private key numbers,[74] the nature of wiretapping makes it possible for the government to monitor encrypted communication without notifying the party being monitored. Although the Clipper Chip idea was eventually abandoned by the Clinton Administration, the debates highlighted the public's desire for some form of checks and balances on the government's accessibility to encrypted communications. Furthermore, critics have since discussed the likely First Amendment, Fourth Amendment, right to privacy and other constitutional violations associated with the possibility of the government mandating the only domestic form of legal encryption.[75]

III. ANALYSIS

Although the Clipper Chip system was abandoned in the midst of public criticism, the government has maintained its interest in promoting similar monitoring mechanisms. Furthermore, the debates surrounding the Clipper Chip have set the stage for concerns regarding other forms of governmentally accessible encryption systems. Abandoning the Clipper Chip system has alleviated the psychological fear of a monitoring mechanism being placed inside the user's computer, but the government still desires the identical accessibility to electronic communications. The government has concentrated its efforts on gaining access through the use of some sort of public key system.[76] As long as the government can access the private keys of individuals in a public key system, the government can monitor their encrypted communications.[77]

---

[72] *See, e.g.*, D.G. Chichester et al., *Tree of Knowledge: Software*, DAREDEVIL, Sept. 1994, at 1.

[73] FDCH, *supra* note 9, at 24 (statements of Dan Geer, Director of Engineering, Open Market, Inc.).

[74] Froomkin, *supra* note 4, at 759-61.

[75] *Id.* at 810-43.

[76] Brock Meeks, *CyberWire Dispatch* (Feb. 22, 1994) (visited Oct. 6, 1997) <gopher://cyberwerks.com/cyberwire/cwd/cwd.94.02.22b>.

[77] *Id.*

A. Current Encryption Policy Choices: Mandatory EES vs. Voluntary EES

Two possible alternatives for the government to maintain accessibility to encrypted communications have emerged after the abandonment of the Clipper Chip. These two alternatives are the implementation of either a mandatory escrowed encryption system or a voluntary escrowed encryption system. An EES is basically a hybrid of a public key system. An EES would utilize the public key and private key mechanisms of a public key system; however, an EES would have the additional characteristic of a third party maintaining a list of each user's private key.[78] Furthermore, an EES must have some sort of mechanism equivalent to the LEAF to enable law enforcement officials to receive the session key which is being used for any particular communication.[79] The third party holding the keys would be known as an escrow agent.[80] A mandatory system would outlaw the use of all forms of encryption technology other than the algorithm associated with the government sponsored EES. A voluntary system would allow users to utilize any form of encryption technology, but would push for the prevalence of the governmentally sponsored EES.[81]

The utility of a mandatory system is to limit the use of other encryption technology to those willing to engage in criminal activity.[82] The distinctive utility of a voluntary system is that it avoids possible constitutional violations created by a mandatory EES.[83] However, if the voluntary EES is merely a means to establishing a mandatory EES, the public should be very concerned with the potential results of opting into that voluntary system. The analysis below discusses prior analyses of a mandatory EES and evaluates the similarities, differences, and implications of a voluntary EES as a precursor to a mandatory EES.

---

78 Froomkin, *supra* note 4, at 759-60.

79 *Id.*

80 *Id.*

81 *Id.* at 796.

82 *See infra* notes 95-97 and accompanying text.

83 *See infra* notes 101-60 and accompanying text.

1. Considerations of a Voluntary Escrowed Encryption System

In contrast to a mandatory EES, a voluntary EES would not outlaw other forms of encryption technology.[84] This would allow users to use other forms of encryption technology, including encryption technology that the government could not decrypt. This obviously frustrates the criminal surveillance justification for the implementation of a voluntary EES.[85] However, many proponents of a voluntary EES argue that this shortcoming can be overcome. Some critics argue that many criminals are simply not very intelligent and would utilize the government sponsored EES to disguise their criminal communications.[86] Others argue that even though criminals may use unmonitorable encryption technology for their criminal communications, they would eventually be forced to communicate within an EES to launder the proceeds from their crimes.[87] Thereafter, law enforcement officials would be able to monitor their activity and search for any patterns of criminal behavior.[88] This latter possibility, however, is predicated on the fact that business and financial institutions would be operating within a governmentally accessible EES. This creates the need for a voluntary EES to establish its prevalence in these markets. In order to satisfy this need, the Clinton Administration has announced that they will try to manipulate the market in order to establish the prevalence of a voluntary EES.[89]

There are several means the government will utilize in order to establish the prevalence of an EES. Through publicity efforts, the government will argue that in order to have a viable encryption infrastructure within the United States, a public key system will be required.[90] Furthermore, the government will argue that it needs to be in charge of the public key system because: 1) it can provide more security than a private entity in charge of individual's private keys; and 2) if left in the hands of industry, only isolated public key systems will emerge, and this will not further the goals of an encryption infrastructure.[91] More

---

[84] *See supra* notes 59-61 and accompanying text.

[85] *See supra* notes 62-70 and accompanying text.

[86] Stewart A. Barker, *Data Encryption: Who Holds the Keys?*, Address before the Fourth Conference on Computers, Freedom, and Privacy (Mar. 24, 1991).

[87] FDCH, *supra* note 9 (statements by Reinsch, Undersecretary for Export Administration) (assuming that financial institutions would operate within a governmentally accessible system and that criminals would attempt to launder criminally acquired money through that system).

[88] *Id.*

[89] *See supra* notes 3-12 and accompanying text.

[90] *See generally* FDCH, *supra* note 9.

[91] Froomkin, *supra* note 4, at 796.

directly, the government will try to establish the prevalence of a voluntary EES through market forces. The market forces which will be utilized are: 1) the government will only use the government sponsored EES so individuals wishing to communicate secretly with the government will have to use that encryption technology; and 2) the government will purchase large quantities of whatever EES hardware and software it decides to sponsor in order to make the price of the equipment feasible for private individuals to utilize.[92]

Whether these incentives will establish the prevalence of a voluntary EES is speculative. There are many critics on opposing sides arguing whether the public will succumb to these influences in light of individual privacy concerns.[93] However, the government's arguments do have significant merit. The most uncontested argument is that some form of standardization will be required in order for a public key system to have any utility. Nonetheless, it is not absolutely necessary for a single public key system to dominate an encryption infrastructure. Industry and the public may desire various public key systems for different purposes. For example, the public may desire one public key system for financial transactions, one or more for industrial and inter-company communications and one for communicating with the government. However, the market will not allow the public to freely determine the desired infrastructure with intentional governmental manipulation of the market. Whether the public will accept a voluntary system for any purpose remains to be seen.

2. Considerations of a Mandatory Escrowed Encryption System

As opposed to a voluntary EES, a mandatory EES would outlaw the use of all encryption technology that the government cannot access. The Federal Bureau of Investigation (FBI) has been the main proponent of a mandatory EES.[94] Proponents of a mandatory EES argue that it is necessary to make an EES mandatory because criminals would otherwise simply use encryption technology that the government could not access.[95] In other words, even if law enforcement officials received a search warrant to wiretap a suspected criminal's telephone line, the officials could not

---

[92] *See generally* FDCH, *supra* note 9.

[93] *Id.*

[94] *See, e.g.*, Louis Freeh, Keynote Luncheon Address at the International Cryptography Institute (Sept. 23, 1994) (stating the FBI's position that a mandatory EES is necessary to serve the purpose of maintaining the agencies ability to monitor criminal communications).

[95] FDCH, *supra* note 9.

decipher the messages that were sent if the user utilized some other form of strong encryption. Furthermore, even if criminals did use the governmentally accessible EES, there would not be any disincentive for criminals to pre-encrypt messages before sending them over the telephone lines.[96]

The utility of implementing a mandatory EES is two-fold. First, the government would be assured access to all electronic communications between law-abiding citizens. Second, if criminals decided to encrypt criminal communications, even though the government may not be able to decrypt those communications, the transmission of those communications would constitute criminal activity. These two characteristics in conjunction would provide a deterrent to prevent criminals from using any form of encryption to hide criminal communications. Simplistically, the government's ability to outlaw the use of any other form of encryption technology outside the governmentally sponsored EES makes the mandatory system superior for furthering the government's criminal surveillance capability.[97] However, the government's ability to outlaw all other forms of encryption technology has been called into question on constitutional grounds.[98] As such, the purpose of this Comment is to expose the public to a significant consideration that should influence their decision; namely, opting into a voluntary EES may have serious constitutional implications if and when the Government attempts to mandate an EES.[99]

B. Potential Results of Opting into a Voluntary EES: Application of the Prevalence of an EES to Constitutional Concerns

Although the Clinton Administration strongly considered mandating an EES, it is presently proceeding to implement a voluntary EES. Whether the Clinton Administration abandoned the idea of a mandatory EES because of the following constitutional concerns is not clear. The administration's abandonment may have been a political decision based on

---

[96] Double-encryption is accomplished by encrypting the plain text of a communication on one's computer and then re-encrypting that communication during transfer to another party with the escrowed encryption algorithm. *Communication and Computer Surveillance, Privacy and Security: Hearing Before the Subcommittee on Technology, Environment and Aviation of the House Committee on Science, Space, and Technology*, 103d Cong., 2d Sess. 56 (1994).

[97] *See infra* notes 139-47 and accompanying text.

[98] *See infra* notes 148-60 and accompanying text.

[99] *See infra* notes 100-160 and accompanying text.

the heated debates that emerged from the advent of the Clipper Chip. Furthermore, it is speculative as to whether the Clinton Administration actually desired the implementation of a mandatory EES as a matter of policy in the first place. However, there is reason to believe that the Clinton Administration does desire the eventual implementation of a mandatory EES. This belief is predicated on the fact that it is questionable whether a voluntary EES will serve the purpose of establishing an encryption infrastructure which would allow the government to monitor encrypted communications, and the fact that the Clinton Administration has announced that it will try to influence the market in hopes of establishing the prevalence of an EES.[100] However, the discussion below is not wholly relevant to whether the current Clinton Administration actually desires the eventual implementation of a mandatory EES; rather, it rests on the possibility that some administration in the future may desire the implementation of a mandatory EES.

The following subsection will outline three constitutional concerns surrounding the implementation of a mandatory EES. The purpose is not to give an exhaustive legal analysis of whether the implementation of a mandatory EES would conclusively infringe on any particular constitutional right. Rather, the issues are presented to show that the immediate implementation of a mandatory EES at least raises these concerns. The question raised is whether it will be easier for the government to circumvent the constitutional issues connected with implementing a mandatory EES after compliance with a voluntary EES establishes the prevalence of that escrowed system. Because of the speculative nature of these arguments, this Section will confine its constitutional analysis within the parameters of and in accordance with the analysis of constitutional issues that Michael Froomkin[101] finds most likely to be violative of the Constitution.[102] Froomkin found that the constitutional protections most likely to be violated by the implementation of a mandatory EES are the First Amendment, the Fourth Amendment, and the Right to Privacy.[103] Froomkin argues that each of these decisions would be based on some sort of balancing of interests that a court would take into

---

[100] *See supra* notes 84-92 and accompanying text.

[101] A. Michael Froomkin is an Associate Professor of Law at the University of Miami School of Law. Froomkin has commented extensively on the legal implications of encryption technology, most notably in *The Metaphor Is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1994).

[102] *See generally* Froomkin, *supra* note 4, at 810-43.

[103] *Id.*

consideration.[104] If the public were to opt into a voluntary EES, these considerations would be significantly altered. In effect, if the public were to opt into a voluntary EES, some of the constitutional protections that are presently enjoyed by the public may be undermined. For each constitutional issue, a summary of Professor Froomkin's analysis, concerning the immediate implementation of a mandatory EES, will be provided. Following each summary, this Comment will illustrate how each analysis would be altered if the government attempted to implement a mandatory EES following prevalent compliance with a voluntary EES.

1. First Amendment Violations

Froomkin argues that the implementation of a mandatory EES may be viewed as compelled speech, creating a chilling effect on speech, and restricting the freedom of association.[105] The individual interests relevant to the First Amendment which are raised by the implementation of a mandatory EES concern personal autonomy.[106] The presence of an escrowed system threatens personal autonomy in two respects. First, users within the system are subject to third parties discovering the source and the content of their encrypted communications.[107] In addition, third parties will be able to observe with whom the user is communicating.[108] Although the government will be required to obtain a search warrant based on some form of probable cause, there still remains the possibility that the private keys will be disseminated outside of the government or subject to governmental abuse.[109]

a. Content-Based Restrictions

The implementation of a mandatory EES can be viewed as compelled speech on two levels. First, individuals in a mandatory EES will be forced to disclose their private keys to the government.[110] Additionally, individuals will be required to disclose a session key, or its equivalent, upon each communication in order for law enforcement officials to

---

[104] *See* discussion *infra* part III.B.

[105] Froomkin, *supra* note 4, at 812-13.

[106] *Id.*

[107] *Id.*

[108] *Id.* at 813.

[109] *Id.* at 813 n.435.

[110] Froomkin, *supra* note 4, at 813 n.435.

maintain their monitoring capability.[111] If viewed as mandatory disclosure, the courts are likely to treat the implementation of a mandatory EES as compelled speech.[112] Compelled speech is viewed as a content-based restriction on speech and receives a strict scrutiny form of review.[113] In order for a law to survive strict scrutiny protection under the First Amendment, the law must: 1) serve a compelling state interest; 2) avoid undue burdens on individuals; and 3) be narrowly tailored to promote the government's interest.[114] Although the government's ability to monitor criminal activity is surely a compelling state interest, there are several considerations as to whether a mandatory EES is narrowly tailored to serving that goal or whether it places undue burdens on the users within that system.[115] Froomkin argues that the escrowed nature of the mandatory EES is probably sufficient to satisfy the narrowly tailored aspect of the test.[116] However, whether the escrowed system would place undue burdens on the public is a value judgment between the interest of the government having the capability of monitoring criminal communications and an individual's burden of operating in a potentially insecure system that is subject to governmental abuse.[117] Furthermore, Froomkin argues that courts will place more weight on interests that are less speculative.[118]

---

[111] *Id.*

[112] *Id.* at 813. The leading case involving mandatory disclosure is *Wooley v. Maynard*, 430 U.S. 705 (1977) (holding it unconstitutional for a state to mandate its citizens to affix license plates which contain the state motto of "Live Free or Die" to their automobiles). However, it is arguable that the implementation of an EES is not compelled speech because there is no public disclosure. Froomkin, *supra* note 4, at 814 (citing Miami Herald Publishing Co. v. Tornillo, 418 U.S. 241, 258 (1974) (holding unconstitutional a state law requiring newspapers to provide a right of reply to political candidates), and West Virginia State Board of Education v. Barnette, 319 U.S. 624, 642 (1943) (finding a compulsory flag salute and recital of the pledge of allegiance unconstitutional)).

[113] *Id.* at 813 (citing Riley v. National Fed'n of the Blind, 487 U.S. 781, 795 (1988) ("Mandating speech that a speaker would not otherwise make necessarily alters the content of the speech")). Froomkin further states in his footnote that "compelled disclosures of fact enjoy the same protection as the compelled expressions of opinion in *Wooley v. Maynard*, 430 U.S. 705, 713 (1977) (holding that requiring cars to display license plates bearing New Hampshire's state motto is unconstitutional) and *West Virginia State Bd. of Educ. v. Barnette*, 319 U.S. 624, 642 (1943) (holding that compelling individuals to recite the pledge of allegiance and salute the flag violates the First Amendment)." *But see* R. George Wright, *Free Speech and the Mandated Disclosure of Information*, 25 U. RICH. L. REV. 475, 496 (1991) (arguing that a less stringent standard would have been more appropriate in *Riley*).

[114] Froomkin, *supra* note 4, at 813 n.436.

[115] *Id.* at 814.

[116] *Id.*

[117] *Id.*

[118] *Id.* at 814 (citing LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 12-24 (2d ed. 1988) (discussing the "public forum" freedom of speech doctrine)).

Froomkin's First Amendment analysis would be significantly altered if the prevalence of an EES is established. Given that the constitutionality of a mandatory EES hinges upon the balancing of governmental and private interests, any extrinsic fact may upset this balance. If and when an EES becomes prevalent in our society, this balance will significantly shift to favor the government's ability to mandate a governmentally accessible EES. The interest in monitoring criminal communications will surely be as significant an interest to the government in the future. However, the burden placed on individuals would arguably be significantly less. First, it will be easier for the government to argue for implementing a mandatory EES when an EES is already in place. The government will simply argue that an encryption infrastructure has been established by the will of the people and that it will be technologically simple to mandate the use of that encryption infrastructure. Second, it will be very difficult for the public to argue that shifting to a mandatory EES is an undue burden when the public itself voluntarily established the prevalence of that system. The public could not argue that they do not want to run the risk of operating in a potentially insecure system when they have voluntarily done so for some time. Furthermore, because courts will place more weight on less speculative interests, if criminals are found to frequently utilize unsupported encryption technology to facilitate crimes, courts in the future will put considerable emphasis on the fact that a mandatory EES is necessary to promote the government's interest. This is an empirical consideration that the government cannot presently rely upon to implement a mandatory EES. However, if this actually occurs after the implementation of a voluntary EES, the balancing of interests will again shift to favor the government.

b. Content-Neutral Restrictions

Even if the implementation of a mandatory system is not viewed as compelled speech, its implementation may be considered as having a chilling effect on speech.[119] The simple fact that people believe that they are being monitored raises this concern.[120] In consideration of the chilling effect that a mandatory EES may create, and in conjunction with the universal application of that system, a mandatory EES could be viewed as

---

[119] Froomkin, *supra* note 4, at 815-17.

[120] *Id.* at 815 (citing, KIM L. SCHEPPELE, LEGAL SECRETS 302 (1988); *see also* SHOSHANA ZUBOFF, IN THE AGE OF THE SMART MACHINE: THE FUTURE OF WORK AND POWER 344-45 (1988) (describing the phenomenon of "anticipatory conformity" among persons who believe they are being observed)).

a content-neutral restriction on speech.[121] If a mandatory EES is viewed as a content-neutral restriction on speech it would have to pass an intermediate level of scrutiny.[122] In order for a law to pass a constitutional intermediate level of scrutiny, a court would have to balance: 1) the likely extent of a chilling effect on speech; 2) any uneven application that the law would place on any particular group; and 3) whether the law left available adequate alternative channels of communication.[123] Furthermore, "because [a] mandatory [EES] directly regulates a mode of speech, the review will be more searching than it would be if the statute had only an incidental effect on speech."[124] Although any attempt to determine the extent of a chilling effect is speculative, the group most affected by its regulation would most predominantly be educated and wealthy people with access to computers.[125] This group has not historically received strong constitutional protection from such regulations because they have access to alternative channels of communications.[126] Froomkin argues that courts would need to balance the government's interest against any undue burden which would be placed on users while making them seek alternative channels of

---

[121] *Id.* (citing Turner Broadcasting Sys., Inc. v. F.C.C., 114 S. Ct. 2445, 2459-62 (1994) (holding that a must-carry provision that distinguished between speakers solely by the technical means used to carry speech is not a content-based restriction); Clark v. Community for Creative Non-Violence, 468 U.S. 288, 293 (1984) (allowing reasonable time, place, and manner restrictions in speech, provided such restrictions are not content-based); City Council of L.A. v. Taxpayers for Vincent, 466 U.S. 789, 804 (1984) (describing an antisign ordinance as content-neutral); Heffron v. International Soc'y for Krishna Consciousness, Inc., 452 U.S. 640, 648-49 (1981) (holding a time, place, and manner regulation on all solicitations at a state fair to be content-neutral)).

[122] *Id.*

[123] *Id.* at 816 (citing City of Ladue v. Gilleo, 114 S. Ct. 2038, 2046 (1994) (applying the balancing test); Clark, 468 U.S. at 293 (same); Consolidated Edison Co. v. Public Serv. Comm'n, 447 U.S. 530, 535 (1980) (same); LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 12-23, at 979 (2d ed. 1988) (stating that the Supreme Court's balancing test examines "the degree to which any given inhibition . . . falls unevenly upon various groups")).

[124] Froomkin, *supra* note 4, at 815 (citing David S. Day, *The Incidental Regulation of Free Speech*, 42 U. MIAMI L. REV. 491 (1988) (discussing the development of the less-exacting incidental regulation doctrine for examining free speech concerns); Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46 (1987) (exploring the nature of content-neutral review); Ned Greenberg, Note, *Mendelson v. Meese: A First Amendment Challenge to the Anti-Terrorism Act of 1987*, 39 AM. U. L. REV. 355, 369 (1990) (distinguishing between regulations that incidentally restrict speech, which are subject to a lower level of scrutiny, and those that directly curtail speech, which are subject to a higher level of scrutiny)).

[125] *Id.* at 816.

[126] *Id.* (citing LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 12-23, at 979-80 (2d ed. 1988) (describing how the Court seeks to avoid upholding communicative limits with a disproportionate impact on the poor, because the poor have the fewest alternative communication channels)). However, even wealthy and educated people may not have access to a truly alternative channel of communication. It is difficult to imagine a form of communication as inexpensive, as potentially anonymous, and as far reaching as encrypted electronic communications.

communication.[127] The relevant constitutional question is whether a mandatory EES "unduly constricts the opportunities for free expression."[128]

Again, Froomkin's First Amendment analysis would be significantly altered if the prevalence of an EES is established. Similar to a content-based focus, the balancing of interests under a content-neutral analysis will significantly shift if and when the public establishes the prevalence of an EES. If viewed as a content-neutral restriction on speech, however, there will be more emphasis placed on whether the public can seek alternative channels of communication. There presently seems to be no alternative form of communication to encrypted electronic communications; however, the public will be hard pressed to argue that the Constitution should guarantee an equivalent to an encryption system that the government cannot access. This is because the public would have shown that it does not mind any burden of governmental accessibility to its communications by establishing and communicating within that system.

c. Freedom of Association

In addition to whether the implementation of a mandatory EES would constitute a content-based or content-neutral restriction on speech, a mandatory EES may also be considered as a restriction on the freedom of association.[129] Encryption technology allows anonymous communications, and anonymity is often a valuable interest surrounding dissident groups.[130] In the interest of protecting the rights of dissident groups, several Supreme Court cases have held that mandatory disclosure of membership lists of dissident groups violates the Constitution.[131] However, this interest may be

---

[127] *Id.* at 816-17.

[128] *Id.* at 817 (citing City of Ladue, 114 S. Ct. at 2045 n.13 (1994) (quoting Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46, 58 (1987)); *see also* Wayte. v. United States, 470 U.S. 598, 611 (1985) (noting that part of the test is whether an "incidental restriction on alleged First Amendment freedom is no greater than is essential to the furtherance of that interest" (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968)))).

[129] Froomkin, *supra* note 4, at 817-21.

[130] *Id.* at 817-18.

[131] *Id.* at 818 n.462 (citing Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 91 (1982) (holding that the "Constitution protects against the compelled disclosure of political associations"); Hynes, 425 U.S. at 623 (Brennan, J., concurring in part) (asserting that a disclosure requirement puts an impermissible burden on political expression); Shelton v. Tucker, 364 U.S. 479, 485-87 (1960) (voiding an ordinance that compelled the public identification of group members engaged in the dissemination of ideas); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) ("It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute . . . restraint on freedom of association . . . ."); Joint Anti-Fascist Refugee Comm. v. McGrath, 341 U.S. 123, 145 (1951) (Black, J., concurring) (expressing the fear that dominant groups might suppress unorthodox minorities if allowed to compel disclosure of

overcome by a compelling state interest.[132] Since the government would have the capability of monitoring with whom any user in a governmentally accessible EES is communicating, the government would in effect be infringing upon the right of a user to freely choose with whom they associate.[133] Although a mandatory EES is unlike published membership lists because the disclosures would not be made until a search warrant had been executed, the intrusion would be more severe because the government would also be able to monitor the content of the communications.[134]

When determining whether a law violates freedom of association, courts will consider the "degree of intimacy" of the communications and whether the communications were conducted "in an atmosphere of privacy" or were communicated in an environment with the intent to "keep their windows and doors open to the whole world."[135] Additionally, courts will find a law unconstitutional if dissident groups can show that there is a "reasonable probability" that disclosure will lead to governmental "threats, harassment, and reprisals."[136] In conclusion, Froomkin argues that courts would refine the constitutional analysis to a balancing of the government's interest of criminal surveillance and any likely threat to dissident groups.[137] Further, courts would be more prone to hold that a mandatory EES violates the freedom of association if its users could show that they were left with

---

associational ties). *But see* Communist Party of the United States v. Subversive Activities Control Bd., 367 U.S. 1, 85 (1961), *reh'g denied*, 368 U.S. 871 (1961) (declining to decide whether forced disclosure of the identities of Communist Party members was an unconstitutional restraint on free association); New York *ex rel.* Bryant v. Zimmerman, 278 U.S. 63, 77 (1928) (holding that a required filing of group member's names with the state constituted a legitimate exercise of police power)).

[132] *Id.* at 819 n.464 (citing Brown, 459 U.S. at 91-92; *see also* Buckley v. Valeo, 424 U.S. 1, 143 (1976) (upholding compulsory disclosure to FEC of names of persons donating more than $10 to campaigns, and public disclosure of contributors of over $100); Griset v. Fair Political Practices Comm'n, 884 P.2d 116, 126 (Cal. 1994), *cert. denied*, 514 U.S. 1083 (1994) (upholding state statute banning political candidates from sending anonymous mass political mailings)). Froomkin notes, "In *McIntyre v. Ohio Elections Comm'n*, 618 N.E.2d 152, 156 (Ohio 1993), *cert. granted*, 114 S. Ct. 1047 (1994), the Ohio Supreme Court let stand a state statute forbidding the circulation of anonymous leaflets pertaining to the adoption or defeat of a ballot issue." *Id.* at 819 n.464.

[133] *Id.* at 819 (citing Board of Directors of Rotary Int'l v. Rotary Club of Duarte, 481 U.S. 537, 548 (1987) (stating that the protections of the First Amendment imply a right to associate); *see also* Citizens Against Rent Control/Coalition for Fair Hous. v. City of Berkeley, 454 U.S. 290, 299 (1981) (holding an ordinance limiting the amount of money that may be contributed to certain political organizations to be an impermissible restraint on free association)).

[134] Froomkin, *supra* note 4, at 820.

[135] *Id.* at 819 (quoting Board of Directors of Rotary Int'l v. Rotary Club of Duarte, 481 U.S. 537 (1987)).

[136] *Id.* at 820 (citing Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 99-101 (1982) (describing "massive" harassment of the Socialist Workers Party by the F.B.I.)).

[137] *Id.* at 820.

no alternative means of communication equivalent to encrypted electronic communications.[138]

Froomkin's freedom of association analysis would also be altered if the prevalence of a sponsored EES is established. The considerations of seeking alternative channels of communication associated with the freedom of speech discussion after the prevalence of an EES are also applicable. Additionally, the prevalence of an EES will significantly form the way in which the public and the courts will look to the nature of an EES. If an encryption infrastructure is created where privacy is the central concern, courts will be more likely to protect freedom of association. However, if the public voluntarily adopts a system in which they know the government has access to every encrypted message, the nature of that infrastructure will change. Ironically, the perception of the encryption infrastructure will begin to resemble a form of communication where one's communications are open to the world. If viewed in this light, a court will not likely protect an individual's freedom of association. In the end, dissident groups may lose a valuable means of furthering their cause while potentially subjecting themselves to governmental threats and harassment.

2. Fourth Amendment Violations

There is no issue whether conducting a wiretap of a private phone line is a search protected by the Fourth Amendment.[139] The government has not proposed that it would not require a search warrant before wiretapping a suspected criminal's communications in an EES. The implementation of a mandatory EES raises the question, however, of whether forcing individuals to disclose their private keys to the government constitutes a search or seizure under the Fourth Amendment.[140] To constitute a search under the Fourth Amendment, individuals must demonstrate that they exhibited a subjective expectation of privacy and that society is willing to accept that expectation as reasonable.[141] The disclosure of keys obviously

---

[138] *Id.*

[139] Froomkin, *supra* note 4, at 826 n.495 (citing United States v. United States Dist. Court (The Keith Case), 407 U.S. 297, 314-21 (1972) (holding that a warrantless wiretap violated Fourth Amendment rights and implicated the First Amendment policies)).

[140] *Id.* at 829.

[141] *Id.* at 827-29 (citing Katz v United States, 389 U.S. 347, 357 (1967) (noting that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment-subject only to a few specifically established and well-delineated exceptions); *cf.* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-59, sec. 103-359, 108 Stat. 3423, 3443-53 (1994) (codified at 50 U.S.C. §§ 1821-1829) (amending FISA to grant the FISA court power to issue *in camera, ex parte* orders authorizing physical searches and

constitutes a search under the Fourth Amendment because individuals would be required to disclose information to the government upon each communication.[142] The purpose of an encryption system is to keep information from being observed by third parties.[143] If an individual is using encryption technology to disguise his communication, he has obviously made efforts to protect himself from observation.[144] Furthermore, society would find this expectation reasonable because the Fourth Amendment has never been interpreted to give the government the right to an effective search, nor required individuals to aid in ensuring an effective search.[145] A mandatory EES may fit within the Fourth Amendment exception of a regulatory search since the EES is "aimed at deterrence of wrongdoing through fear of detection."[146] However, regulatory searches have rarely been upheld in connection with the search of one's home and Froomkin concludes that a mandatory EES would not fall within this exception, at least in connection with the use of private individuals for noncommercial purposes.[147]

The prevalence of an EES would have a drastic impact upon Froomkin's Fourth Amendment analysis. If a voluntary EES has established its prevalence through public acceptance, an individual could not argue that he or she has a subjective expectation of privacy in his or her communications. Through compliance with a voluntary EES, individuals could not argue that they have a subjective expectation in communications which they knowingly transmitted using a system to which they know the government has access. Furthermore, an individual could not argue that society should find that expectation reasonable when the public has taken affirmative steps to ensure the government has access to its communications. Although the courts have never suggested that the government has a right to an effective search, nor that the public must help them perform an effective search, the fact that the public has voluntarily done so will demonstrate that society finds it reasonable for people to be required to operate in a governmentally accessible system.

"examination of the interior of property by technical means" on a lesser showing of need than would be required for a warrant); Benjamin Wittes, *Surveillance Court Gets New Power*, LEGAL TIMES, Nov. 7, 1994, at 1 (noting the ACLU's claim that the extension of FISA court's power is "a clear violation of the Fourth Amendment")).

[142] *Id.* at 829.

[143] *Id.*

[144] Froomkin, *supra* note 4, at 829.

[145] *Id.* at 826.

[146] *Id.* at 830 (quoting Craig M. Cornish and Donald B. Louria, *Employment Drug Testing, Preventative Searches, and the Future of Privacy*, 33 WM & MARY L. REV. 95, 98 (1991)).

[147] *Id.* at 832-33.

3. Right to Privacy

The constitutional concept of the right to privacy gained historical recognition in *Roe v. Wade,* where the Supreme Court stated that many provisions in the Bill of Rights create a synergistic penumbra of rights.[148] The right to privacy has since evolved into three different categories: 1) the right to be left alone; 2) the right to autonomous choice regarding intimate matters; and 3) the right to autonomous choice regarding other personal matters.[149] The simple notion of mandating an EES naturally infringes on all three rights.[150] Furthermore, Froomkin states that the right to privacy promises to be the "most fertile area for legal adaptation to the new challenges posed by increasing state surveillance power and compensating private responses such as [encryption]."[151] However, the right of privacy infringements will be held constitutional as long as they are sufficiently related to a compelling state interest.[152]

Froomkin argues that issues regarding the right to autonomy concerning non-intimate matters will usually be protected by single provisions of the Bill of Rights, but there are distinctive characteristics of the right to be left alone and the right to autonomy regarding intimate matters that distinctively relate to the implementation of a mandatory EES.[153] A subset to the right to be left alone is the right to informational privacy.[154] This right was recognized in *Whalen v. Roe* where the court

---

[148] *Id.* at 838 (citing Roe v. Wade, 410 U.S. 113, 152 (1973) (relying on penumbras in the Bill of Rights); *cf.* Griswold v. Connecticut, 381 U.S. 479, 499-500 (1965) (Harlan, J., concurring) (stating that privacy derives not from penumbras in the Bill of Rights, but from fundamental ideas of ordered liberty)).

[149] Froomkin, *supra* note 4, at 838 (citing TRIBE, *supra* note 126, at 15-1; Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1340 (1992)). Froomkin further states, "For an argument that the three strands of the right to privacy are actually inimical to each other, at least in the eyes of their advocates on the Supreme Court, *see generally* David M. Smolin, *The Jurisprudence of Privacy in a Splintered Supreme Court*, 75 MARQ. L.REV. 975 (1992). Froomkin, *supra* note 4, at 838 n.557.

[150] Froomkin, *supra* note 4, at 838.

[151] *Id.*

[152] *Id.*

[153] *Id.* at 838-43.

[154] Froomkin, *supra* note 4, at 839-40 n.563 (citing Francis S. Chlapowski, Note, *The Constitutional Protection of Information Privacy*, 71 B.U. L. REV. 133, 154-55 (1991) (concluding that because most theories of personhood assume personal information is a crucial part of a person's identity, there must be a recognized "right to [informational] privacy . . . based on personhood" and that information is property protected by the Fifth Amendment); Gary R. Clouse, Note, *The Constitutional Right to Withhold Private Information*, 77 NW. U. L. REV. 536, 541-47 (1982) (tracing the development of the right to informational privacy, and noting that the Supreme Court's use of a balancing test to determine whether an individual's constitutional rights have been infringed by a government-mandated disclosure of information)).

found that there was an individual privacy interest when a law mandated patients receiving certain prescription drugs be placed on a government list.[155] Although the court found that this statute was narrowly tailored to a compelling state interest, the court warned that a law may be found unconstitutional if the government were to amass large quantities of information not necessarily related to a compelling state interest.[156] The implementation of a mandatory EES may approach this line.[157] The right to autonomous choice regarding intimate matters relates to an individual's choice regarding "marriage, procreation, contraception, family relationships, and child rearing and education."[158] Because secrecy is a prerequisite for familial autonomy, encrypted communications between family members might invoke this right.[159] Furthermore, Froomkin argues that the utilization of encryption technology may eventually become a common means of establishing and maintaining familial relationships and could eventually present a strong case that a mandatory EES could violate this right.[160]

The prevalent establishment of a governmentally accessible EES will alter Froomkin's analysis of the right to information and the right to

---

[155] *Id.* at 839-40 (citing Whalen v. Roe, 429 U.S. 589, 598-99 (1977) (acknowledging the existence of the right, but finding that it could be overcome by a narrowly-tailored program designed to serve the state's "vital interest in controlling the distribution of dangerous [prescription] drugs"); *see* Gary R. Clouse, Note, *The Constitutional Right to Withhold Private Information*, 77 NW. U. L. REV. 536, 547-57 (1982) (collecting and dissecting inconsistent circuit court cases dealing with the right to withhold private information)).

[156] *Id.* (citing *Whalen*, 429 U.S. at 601-04). However, the *Whalen* court specifically declined to decide the issue. 429 U.S. at 605-06.

[157] Froomkin, *supra* note 4, at 840.

[158] *Id.* at 841 n.570 (citing Paul v. Davis, 424 U.S. 693, 713 (1976); *see also* Roberts v. United States Jaycees, 468 U.S. 609, 618-22 (1984) (describing types of "personal bonds" and relationships entitled to heightened constitutional protection); Moore v. City of E. Cleveland, 431 U.S. 494, 499 (1977) (plurality opinion) (recognizing a right to choose which relatives to live with); Roe v. Wade, 410 U.S. 113, 152 (1973) (protecting the reproductive decisions of women); Doe v. Bolton, 410 U.S. 179, 197-98 (1973) (recognizing the right to make reproductive decisions without interference from a hospital committee); Eisenstadt v. Baird, 405 U.S. 438, 452-55 (1972) (protecting the procreative decisions of unmarried opposite-sex couples); Loving v. Virginia, 388 U.S. 1, 12 (1967) (endorsing the right to engage in an interracial marriage); Griswold v. Connecticut, 381 U.S. 479, 482-86 (1965) (establishing the right of married opposite-sex couples to make procreative decisions); Poe v. Ullman, 367 U.S. 497, 551-54 (1961) (Harlan, J., dissenting) (arguing that the Constitution protects the procreative decisions of married opposite-sex partners); Skinner v. Oklahoma, 316 U.S. 535, 541 (1942) (recognizing the right not to be sterilized); Pierce v. Soc'y of Sisters, 268 U.S. 510, 534-35 (1925) (holding that parents have the right to determine the schooling of their children); Meyer v. Nebraska, 262 U.S. 390, 399-400 (1923) (recognizing a parental right to determine what language children may learn); Kenneth L. Karst, *The Freedom of Intimate Association*, 89 YALE L.J. 624, 637-38 (1980) (arguing that divorce—the freedom of disassociation—is a fundamental privacy right)).

[159] Froomkin, *supra* note 4, at 842.

[160] *Id.*

privacy concerning intimate matters in two respects. First, as with the undue burden analysis concerning the freedom of speech and association, the public will have demonstrated its approval of the government having access to its communications. Second, as a corollary to the first point, immediate compliance with a voluntary EES will thwart any attempt to establish the perception of encryption technology as a means of maintaining personal relationships. An individual could not argue that he or she has become reliant upon a governmentally accessible EES to maintain familial relations and that this right will be destroyed simply because it now has no alternative form of encryption system to utilize.

IV. CONCLUSION

If and when the prevalence of a governmentally accessible EES is voluntarily established, it is easily foreseeable that a future administration may wish to take the next step and mandate a governmentally accessible EES to thwart the criminal secrecy that the voluntary EES has not been able to monitor. As illustrated above, the government can argue that it is in the interest of the public, and that the public has shown that it is willing to accept the loss of some freedom to accomplish this goal. This could be argued even if the true reason for the prevalence of a governmentally accessible EES is accomplished through governmental market manipulation and the propagated fear that only the government could establish a secure system.

The purpose of this Comment is not necessarily to choose for the public whether it should or should not opt into the implementation of a voluntary EES. But, as this Comment illustrates, the consequences may have a dramatic constitutional impact on the public's rights, not to mention the rights of those who did not wish to opt into any voluntary scheme. History has proven that constitutional notions of liberty change over time. The government has often played a significant proactive role in forming those notions. Encryption technology has not yet played an important role in public life, but as the technological age is increasingly forming the environment in which our society operates, the potential prevalent use and consequences of encryption technology should not be treated summarily. Although business and industry will probably play a more important role in forming the necessities of encryption technology and the requisite infrastructure, individuals should also be concerned in the private use of encryption. This is where constitutional issues will be the most sensitive. In conclusion, the public should take a serious look at how encryption technology should be used to benefit our society and determine what role the government should play. The public should not venture blindly into the

future only to find out that it has no other choice than to accept an information infrastructure where the government can mandate access to all electronic communications. Furthermore, with increasing technological ability to amass large quantities of data, every American citizen's communication equipment may facilitate the "memory holes" that George Orwell envisioned.