UIC John Marshall Journal of Information Technology & Privacy Law

Volume 18
Issue 3 *Journal of Computer & Information Law - Spring 2000*

Article 6

Spring 2000

Big Brother Is at Your Back Door: An Examination of the Effect of Encryption Regulation on Privacy and Crime, 18 J. Marshall J. Computer & Info. L. 825 (2000)

Hillary Victor

BIG BROTHER IS AT YOUR BACK DOOR: AN EXAMINATION OF THE EFFECT OF ENCRYPTION REGULATION ON PRIVACY AND CRIME

> The hypnotic eyes gazed into his own. It was as though some huge force were pressing down upon you-something that penetrated inside your skull, battering against your brain, frightening you out of your beliefs, persuading you, almost, to deny the evidence of your senses. In the end the Party would announce that two and two made five, and you would have to believe it.
>
> George Orwell[1]

I. INTRODUCTION

The United States Constitution serves as a foundation providing Americans with an opportunity to shape their identity in response to changing societal norms and conditions.[2] The Founding Fathers drafted the Bill of Rights with an eye to protect individual rights.[3] Specifically, the Fourth Amendment protects individuals from unreasonable government intru-

1. GEORGE ORWELL, 1984, at 68-69 (1949). *See also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1656-57 (1999). Orwell describes the "telescreen" which continuously broadcasts propaganda, providing state officials, known as the "Thought Police," with incessant surveillance over individuals. *Id.* This telescreen is similar to a computer with Internet access. *Id.* Orwell envisioned Big Brother, the leader of the state of Oceania who watched over individuals of the state, as the threat to individual privacy. *Id. See also* Brian J. Serr, *Great Expectations Of Privacy: A New Model For Fourth Amendment Protection*, 73 MINN. L. REV. 583, 583-84 (1989). Orwell's novel envisions a society without individual privacy or Fourth Amendment rights. *Id.* Big Brother's continuous surveillance depicted a society without constitutional limitations on governmental intrusion. *Id.* Orwell's novel presented two sides in conflict with one and other, the citizens who longed for privacy and the government who claimed their need for surveillance and intrusion. *Id.* In Orwell's novel, the conflict desisted with a victory for the government, but at the cost of individual freedom for citizens. *Id.*

2. *See* WILLIAM R. SANFORD, PH.D. & CARL R. GREEN, PH.D., BASIC PRINCIPLES OF AMERICAN GOVERNMENT 72-74 (1986). *See also* JAMES W. DAVIDSON & MARK H. LYTLE, THE UNITED STATES: A HISTORY OF THE REPUBLIC 155-57 (ann. tchrs. ed. 1988).

3. *See* SANFORD & GREEN, *supra* note 2, at 312-322 (providing an overview of the individual rights guaranteed under the first ten amendments); *see also* DAVIDSON & LYTLE, *supra* note 2, at 165-67.

sion.[4] The prospect of Big Brother watching over people and controlling their thoughts would have been disconcerting to our Founding Fathers.[5] A preferable image of the citizen in a free society can be found in Orwell's character, Winston, who articulates freedom from government control by writing "freedom is the freedom to say that two plus two make four."[6] The tradition of freedom from government control is fundamental to the United States ("U.S.") historical experience.[7] Puritans wanted the freedom to worship in a manner different from the one allowed by the English government.[8] In search of independence from the critically watchful eye of a government limiting free expression, the Puritans left England for America.[9] Seeking to provide freedom, yet recognizing the need for some control, our Founding Fathers established the Constitution's framework of laws to guide the nation.[10]

With the new and developing communication technology of the Internet,[11] Fourth Amendment interpretation must be reviewed in light of the impact cyberspace[12] has on society.[13] This interpretation takes on further significance when one considers the pervasive nature of cyber-

4. *See* U.S. CONST. amend. IV (providing for "[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 be issued, but upon probable cause . . . .").

5. *See generally* ORWELL, *supra* note 1, at 68-69.

6. *Id.* at 69.

7. *See* SAMUEL ELIOT MORISON, THE OXFORD HISTORY OF THE AMERICAN PEOPLE 55 (4th ed. 1965).

8. *See id.*

9. *See id.*

10. *See* U.S. CONST. preamble.

11. *See* Shea v. Reno, 930 F. Supp. 916, 925-26 (S.D.N.Y. 1996), *aff'd* without op., Reno v. Shea, 521 U.S. 1113 (1997) (defining the Internet as a collection of independent networks linking host computers worldwide to provide public content to individual computers); *see also* American Libraries Association v. Pataki, 969 F. Supp. 160, 164 (S.D.N.Y. 1997) (defining the Internet as a "global communications medium linking people, institutions, corporations, and governments . . . across the world . . . capable of rapidly transmitting communications.").

12. *See* Cyberspace v. Engler, 55 F. Supp.2d 737, 743 (E.D. Mich. 1999) (explaining that the Internet is comprised of the World Wide Web which "allows users to publish documents, also called 'Web pages,' that can then be accessed by any other user in the world."). Internet users can obtain Web contents by typing in the specific address ("URL") using a "search engine," and "linking" between Web pages. *Id.* The Internet and World Wide Web make up Cyberspace. *Id.*; *cf.* Ian C. Ballon, *The Emerging Law Of The Internet*, 547 PLI/PAT 169, 177 (1999) (providing the history of the term "Cyberspace"). Cyberspace was a term coined in William Gibson's science fiction short story "Burning Chrome," published in 1987. *Id.* A world where people interacted with computers, transacted business through computers, and used computers to provide entertainment was depicted in Gibson's subsequent novel, "Neuromance." *Id.*

13. *See Shea*, 930 F. Supp. at 926. As of 1996, as many as forty million individuals had Internet access, and by 1999, this number was anticipated to reach 200 million. *Id.*

space as an informational and educational tool,[14] a communication link within companies,[15] a commercial tool,[16] and a low-cost form of entertainment.[17] In this age of rapidly developing technology, the image of Big Brother and the Orwellian notion of "doublethink,"[18] the power of holding two contradictory beliefs in one's mind contemporaneously and accepting both,[19] give one cause to approach the future with caution.

The quintessential right to privacy embraced by our Founding Fathers endures in the age of cyberspace.[20] Communications and information are encrypted to protect privacy in cyberspace.[21] The current encryption debate[22] is a prime example of "doublethink."[23] While necessary to preserve national security,[24] commercial transactions,[25] and personal privacy,[26] encryption also allows criminals to act under a veil of

14. *See id.* (noting that educational institutions, libraries, and communities maintain computer networks linked to the Internet); *see also* Reno v. ACLU, 521 U.S. 844, 850-51 (1997) (noting that many higher educational institutions provide free Internet access).

15. *See Reno*, 521 U.S. at 850-51 (noting that corporations link employees to the Internet through inter-office networks).

16. *Pataki*, 969 F. Supp. at 173. The Internet serves as a "conduit for transporting digitized goods," including software, data, music, graphics, and videos. *Id.*

17. *See Shea*, 930 F. Supp. at 927. Computer coffee shops employ the Internet as commercial tool providing access to customers at an hourly fee. *Id. See also Reno*, 521 U.S. at 850-51.

18. Marianne Lavelle, *Next Rights Battle Is Going Online: Infonauts Say Cybercops Trample Speech, Assembly, and Other Rights*, NAT'L L.J., July 25, 1994, at A1 (noting that Internet communications are growing and will top one billion in the twenty-first century).

19. *See* Erich Fromm, *Afterword* to GEORGE ORWELL, 1984, at 264 (New American Library of World Literature 1961) (1949).

20. Olmstead v. U.S., 277 U.S. 438, 478 (1928). Justice Brandeis' dissent stated the right to privacy is "the most comprehensive of rights and the right most valued by civilized men." *Id.*

21. *See* H.R. REP. No. 105-108 (V), pt. 3, at 3 (1997) (defining encryption as the process of scrambling information into code language unreadable to anyone other than the intended recipient of the information).

22. *See id. See also* 145 CONG. REC. E297 (daily ed. Mar. 1, 1999) (statement of Hon. Goodlatte, Representative from Virginia) (discussing personal privacy under the Security and Freedom through Encryption (SAFE) Act of 1999).

23. *See* Fromm, *supra* note 19, at 264.

24. 144 CONG. REC. S9419 (daily ed. July 30, 1998) (statement of Mr. Lott of Americans for Computer Privacy) (explaining encryption affects all Americans because it is essential to protect the national infrastructure including "the power grid, telecommunications infrastructure, financial networks, air traffic control operations, and emergency response systems.").

25. *See id.* Encryption protects a company's confidential information from getting into the wrong hands. *Id.* Companies often encrypt employee salary information, trade secrets, target market analysis, and information about competitors. *Id.*

26. *See id.* Encryption is used in the interest of private citizens. *Id.* Encryption protects credit card numbers from being obtained when purchasing goods on-line, ensures the security of patient medical records stored in hospital databases, and promotes the confidentiality of tax information transmitted to the IRS. *Id.* Private individuals using e-mail to

protection.[27] The government argues that it is in the interest of national security to strengthen the ability for law enforcement to obtain information by regulating the use of encryption[28] and that the Cyberspace Electronic Security Act ("CESA") is the best means of accomplishing this goal.[29] However, privacy advocates express concern about the methods CESA will employ to regulate encryption, since CESA may violate Fourth Amendment rights.[30] Privacy advocates contend that CESA is the government's means of taking on a Big Brother role.[31]

This Comment examines the continuing struggle between the U.S. government's desire to regulate encryption and the American citizen's desire to keep their personal information private from the watchful eye of the federal government.[32] The future of cyberspace security through encryption regulation and the impact CESA will have on privacy and crime are also discussed. This Comment examines the dilemma inherent in the regulation of cyberspace by providing a brief background of encryption including its benefits and drawbacks, delineating the fruitless history of similar legislation providing for decryption tools, and explains the difference between privacy and the right to privacy. This Comment analyzes the policy and text of CESA, together with the legal issues re-

---

communicate with friends, family, and loved ones use encryption to keep their private lives confidential. *Id.*

27. *See Preserving America's Privacy And Security In The Next Century: A Strategy For America In Cyberspace: A Report to the President of the United States* [hereinafter *The Clinton Administration's White Paper*] (Sept. 16, 1999) (explaining that the majority of people use encryption for legitimate and lawful security reasons). However, encryption is also used by criminals to conceal their unlawful activities. *Id.* § 3.

28. *See id.* (explaining the need for and use of strong encryption for security in corporate, governmental, and personal arenas, warranting stronger law enforcement tools to handle issues arising from harmful uses of encryption). While existing law allows law enforcement officials to collect evidence of criminal activity through wiretaps, wiretaps are insufficient to tackle the threat criminals pose to the U.S. in Cyberspace. *Id.* § 4. Further, because encryption is unreadable even if seized, unregulated encrypted communications facilitate criminal activity in Cyberspace. *Id.* Therefore, the government argues that some form of regulation is necessary to ensure the security of American citizens. *Id.*

29. *See generally* Cyberspace Electronic Security Act of 1999 [hereinafter CESA] (last modified Sept. 17, 1999) <http://www.cdt.org/crypto/CESA/CESArevised.shtml> (providing the complete text of CESA). Pres. William J. Clinton presented this proposed legislation to Congress while the House/Senate was proceeding on impeachment charges against the President. Consequently, the House and Senate accepted the proposal from the President and gave it a document number, however, neither house gave the legislation a bill number or read the proposed legislation into the record.

30. *See Justice Dept. Seeks New Encryption-Related Authority,* Comm. Daily, Aug. 20, 1999, *available in* 1999 WL 7580219.

31. *See* Wayne Rash, *Justice Dept.'s Proposal Threatens Your Privacy*, COMMUNICATIONS WEEK, Sept. 6, 1999, at 62 (comparing acts of law enforcement officials permitted under CESA to the black bag jobs in paperback spy novels and the actions of the Soviet Union's KGB).

32. *See* ORWELL, *supra* note 1, at 68-9.

solved by CESA, concerns about CESA's effectiveness, and the ways in which the proposed legislation encourages the government to take on a Big Brother role. Redrafting and narrowly tailoring CESA to promote its goals while protecting the privacy of Americans is proposed. This Comment argues that by redrafting and narrowly tailoring CESA, the federal government can achieve its goals while protecting the privacy rights of law-abiding American citizens without taking on the role of Big Brother.[33]

II. BACKGROUND

I shot an arrow into the air; it fell to the earth I know not where.[34]

The jurisdictional nature of the law is rooted in geography.[35] The concept of cyberspace jurisdiction is one such example. Cyberspace is a unique place where people communicate through interconnected computers.[36] As a result, it cannot be defined in terms of spatial parameters previously known to American society or the law.[37] Therefore, some form of federal regulation is essential to ensure national security, commercial security, and personal privacy. It is equally important to ensure that the means of national regulation does not provide excessive power to law enforcement officials, a condition that might inhibit the growth of cyberspace.[38] CESA recognizes the need for such balancing.[39] Before

33. *See The Clinton Administration's White Paper*, *supra* note 27, § 4, I (explaining the government's need for and goal of creating stronger law enforcement tools and regulations to deal with harmful issues arising from criminal use of encryption).

34. *See* American Libraries Association v. Pataki, 969 F. Supp. 160, 167 (S.D.N.Y. 1997) (noting the poetry of the anonymity and borderless world of cyberspace).

35. *See id.* at 169.

36. *See* Shea v. Reno, 930 F. Supp. 916, 922 (S.D.N.Y. 1997) (explaining that via the Internet, the world is confronting a more divergent communications medium than any previously established).

37. *See Pataki*, 969 F. Supp. at 168. The "borderless world of the Internet raises profound questions" about the relationship between states and the relationship between individual states and the federal government. *Id. See also* Rob Reilly, *Conceptual Foundations of Privacy: Looking Backward Before Stepping Forward*, 6 RICH J.L. & TECH 6, *2 (1999) (explaining that the walls of privacy protection allowing individual seclusion have been removed by the World Wide Web). The crumbling of these walls erodes the assurance of privacy, even within the confines of an individual's home. *Id.* With the rapid developments in technology, privacy is more difficult to protect and easier to violate. *Id. See also* Jerry Berman & Deidre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 551, 556 (1999) (explaining that the lack of definite boundaries and inherent international scope makes exercising government authority over cyberspace difficult at best).

38. *See Pataki*, 969 F. Supp. at 169 (noting that the Internet "must be marked off as a national preserve to protect users from inconsistent legislation" that, if excessive, could inhibit Internet development).

39. *See* CESA, *supra* note 29, § 102(a-f) (recognizing that as commerce is moving into cyberspace, there is a growing demand for electronic commerce and information access by private citizens, merchants, manufacturers, companies, service providers, banks, govern-

the encryption debate and proposed legislation can be analyzed, it is necessary to examine the terms central to this debate. Specifically, this comment will define encryption and review the history surrounding the encryption privacy debate.[40]

A. ENCRYPTION

Encryption is the method of concealing a message, using either a code or a cipher so that only the intended recipient, or someone with the proper key, is able to read the message upon delivery.[41] Encryption is a means of protecting data security and personal privacy of data when communicating in cyberspace.[42] The benefits of encryption are most ob-

---

ments of all levels, and educational institutions). This increasing demand and reliance on cyberspace expands the risks to private citizens and institutions alike. *Id.* The need to curb these risks and allow cyberspace to achieve its potential has been met by the technology industry through encryption providing confidentiality of data and communications. *Id.* The drawback of this confidentiality is the increased risk of criminal activity. *Id.*

40. *See* Zhonette M. Vedder-Brown, *Government Regulation of Encryption: the Entry of "Big Brother" or the Status Quo?*, 35 AM. CRIM. L. REV. 1387, 1403-04 (1998) Explaining that privacy from a moral standpoint, is different than the right to privacy protected under the Fourth Amendment. *Id.* Physical privacy includes "seclusion, solitude, security, or bodily integrity, at home and elsewhere." *Id.* "Informational privacy includes confidentiality, secrecy, or anonymity, especially with respect to correspondence, conversation and records." *Id.* America values its independence, as do American citizens. *Id.* This value of independence is promoted through the ability to think freely, avoid uniformity, and engage in "voluntary seclusion." *Id.* The privacy concept promoted by this definition is that of moral privacy. *Id.* The Fourth Amendment itself and subsequent case law interpreting the Fourth Amendment's right to privacy define an individual's right to legal and procedural privacy. *Id.*

41. *See* A. Michael Froomkin, *The Metaphor Is The Key: Cryptography, The Clipper Chip, And The Constitution*, 143 U. PA. L. REV. 709, 713 (1995) (explaining the difference between codes and ciphers used in encryption). Codes are an established arrangement of symbols that hold meaning constructing a communication dialectic. *Id.* For example, "Paul Revere's 'one, if by land, and two, if by sea' was a code." *Id.* Most modern cryptography uses ciphers. *Id.* at 714. The language that is used in ciphers is "plaintext." *Id.* Plaintext describes the original message that will be converted through encryption. *Id.* "Cipher text" is the resulting converted counterpart of "plaintext." *Id.* Cipher text is merely a mathematical algorithm applying a key used by the sender to encrypt a message into code language, and used by the receiver to decrypt the code language revealing the message. *Id.* There are two types of keys that can be used in the encryption process using cipher text, the private key and the public key. *Id.* A private key system is one where both the sender of the message and the receiver use the same key to encrypt and decrypt the message. *Id.* A public key system is one where the sender of the message uses one key to encrypt the message and the receiver of the message uses another key to decrypt the message. *Id.* Although a third party recovery agent may hold a decryption key, only the intended recipient should be allowed to decrypt private information. Privacy should protect the expectations of the sender of the information, not the government or third parties.

42. *See id.* at 719. Encryption can contribute to the security of data and privacy of communications. *Id.* The government endorses the benefits of cryptology, which is the art of encryption. *Id.* Encryption comforts lawyers, banks, and others who have a duty to

vious in commerce and industry.[43] However, personal benefits are also evident.[44]

Inherent in any technology are evils coexisting with benefits; such is the case with encryption.[45] Encryption is used by offenders to facilitate criminal activities and hide their identities from the government.[46] It is

---

secure the confidentiality of communications. *Id.* There is a need to encourage the development of encryption to ensure the continuing development of Cyberspace, electronic commerce, and information systems. *Id.; see also* Vedder-Brown, *supra* note 40, at 1403 (explaining that encryption provides national security, commercial security, and personal privacy).

43. *See* Froomkin, *supra* note 41, at 719 (explaining that banks worldwide use encryption to protect against forgery, to protect ID numbers used in automated teller transactions, and to prevent crimes arising from "digital cash" transactions). The U.S Department of the Treasury mandates the use of encryption of all transfer messages dealing with U.S. electronic funds. *Id.* at 719-20. Telebanking relies on encryption to ensure customers that their transactions remain private. *Id.* at 720-21. U.S. corporations rely on encryption to secure market information, research and development, trade secrets, and to prevent industrial espionage by both domestic and foreign competitors. *Id.* at 722-23. Lawyers are increasingly relying on encryption to prevent confidential attorney-client communications from reaching third parties. *Id.* at 724. If this confidential communication is overheard or received, even unintentionally by a third party, the attorney-client privilege may be waived, thus affecting the outcome of litigation. *Id.* at 724-25. Businesses using cellular telephones, telephones, fax machines, and e-mail rely on encryption to maintain confidentiality also. *Id.* at 728-29.

44. *See id.* at 730. The average citizen wanting to hide information or private communications seems trivial in comparison to the benefits of encryption for industry. *Id.* Encryption allows an individual to experience a sense of security knowing that their diary, love letters, or plans for a surprise are only accessible to the holder of the decryption key. *Id.*

45. *See id.* at 727. The negative aspect of encryption is its ability to disguise criminal communications, records, and identities. *Id.* As a result of President Reagan's War on Drugs, law enforcement officials turned to surveillance, wiretapping, and informants because they lacked the legal and technological abilities to seize encrypted data and decrypt it. *Id.* at 857-58.

46. *See* Vedder-Brown, *supra* note 40, at 1399 (explaining that the best evidence of a computer crime is most likely found on a computer). The use of encryption by criminals acts as a bar to evidence of criminal activity unless law enforcement officials possess a decryption key allowing them to reveal the plaintext of information or communications. *Id.* Criminal activity against children is frequently facilitated by encryption. *Id.* This criminal conduct includes pornography, the Internet transmission of pornography to children, kidnapping, rape, and harassment. *Id.* Encryption becomes a problem for law enforcement officers when an individual is suspected of committing a crime and encryption hides the identity of the alleged offender. *Id.* Internet harassment against adults has also been masked by encryption. *Id.* An e-mail message sent to President Clinton threatening to "blow [his] head off" is one such example. *Id.* at 1400. Disgruntled employees have also used encryption to embezzle money and law enforcement officers have prevented law enforcement officers from accessing evidence of the embezzlement because they did not have a decryption key. *Id.* Encryption has also facilitated Internet scams including the theft and sale of credit card numbers by hackers. *Id.* The criminal selling of individuals' private criminal, employment, and credit records has also been masked through encryption. *Id.* at

this criminal use of encryption that CESA seeks to prevent.[47] However, history shows that even when law enforcement has had access to the plaintext of encrypted information, tragedies still occur. For example the World Trade Center bombing was not prevented, and criminals such as Timothy McVeigh and the Unabomber, were not apprehended even though law enforcement had access to plaintext data.[48]

B. THE HISTORY OF FEDERAL GOVERNMENT SURVEILLANCE OVER ELECTRONIC TECHNOLOGY

The Bush Administration began the process of ensuring government access to telephone conversations via electronic surveillance through digital telephony legislation signed into law on October 25, 1994, as part of the Communications Assistance for Law Enforcement Act ("CALEA").[49] It was through this legislation that the government established its presence in the electronic technology debate.[50] The digital telephony legislation established the government's ability to seize any information transmitted over the telephone wires without notice if it reasonably believes notice will result in the destruction of evidence.[51] The next at-

1401. Furthermore, terrorists and foreign spies endanger national security by using encryption to conceal their plans. *Id.* While many other potential crimes could be facilitated by encryption, these offenses serve as examples of the impact advancing encryption technology has on crime. *Id.*

47. *See* CESA, *supra* note 29, § 102(f)-(h) (recognizing that encryption is a double-edged sword, important in protecting the privacy interests of lawful communications, but contemporaneously used by criminals to facilitate their activities). It is this unlawful use of encryption by criminals that threatens public safety and challenges law enforcement officials. *Id.* Even if law enforcement officials can intercept encrypted evidence of crimes, technology does not presently allow the decryption of encrypted information without a key. *Id.* The government urges that time is of the essence in stopping criminal activity before a tragedy occurs. *Id.* Without the means of decrypting evidence into a plaintext version, computer evidence of crime is virtually useless. *Id.* The government contends that allowing law enforcement officers access to the plaintext of criminal evidence far outweighs the need for law-abiding citizens to keep their information confidential through encryption. *Id.*

48. *See* ACLU, *Big Brother In The Wires: Wiretapping In The Digital Age* (An ACLU Special Report) (Mar. 1998).

49. *See* Pub. L. No. 103-414, 108 Stat. 4279, 4280 (1994) (codified at 47 U.S.C.A. §§ 1001-1010 (1999) (requiring that law enforcement officers be provided with access to digital telephony by telecommunications common carriers to aid law enforcement officials in their wiretapping duties).

50. *See* Dena R. Klopfenstein, Comment, *Deciphering The Encryption Debate: A Constitutional Analysis Of Current Regulations And A Prediction For The Future*, 48 EMORY L.J. 765, 774 (1999).

51. *See id.* at 776 (explaining the exceptions to the general rule that notice is required for a valid search and seizure); *see also* Nan Hunter, et al., *Contemporary Challenges To Privacy Rights*, 43 N.Y.L. SCH. L. REV. 195, 204 (1999) (Nadine Strossen explains that CALEA forces telecommunications industries to facilitate government surveillance by modifying their telecommunications equipment). CALEA is like requiring that mandatory

tempt came with the Clinton Administration's proposed Clipper Chip, mandating a "back door" to computers and software to allow law enforcement officials to skirt encryption.[52] The initial Clipper Chip proposal and its revised version did not pass due to Fourth Amendment concerns.[53] Consequently, encryption product use is currently regulated through executive orders.[54] Decryption of encrypted data is provided for in one federal statute, which explains that third parties are not responsible for ensuring the government's ability to decrypt data unless the encryption was provided by a third party and this third party possesses the necessary decryption key.[55] However, current orders do not provide law enforcement officials with a means of decrypting encrypted data when a third party does not hold a key.[56]

C. A New Means Of Regulation

1. *Encryption Debate Justifies Regulation*

While there are arguments on both sides of the encryption debate, neither side is pleased with the current means of regulating encryption through executive order.[57] Law enforcement agencies advocate an encryption regulation program providing for the authority and means of decrypting encrypted information.[58] Privacy advocates, civil libertarians, and the software industry advocate more relaxed encryption regula-

---

bugs be placed in the walls of apartments and homes by the construction industry pursuant to a government mandate with the purpose of facilitating government surveillance over citizens. *Id.*

52. *See* Klopfenstein, *supra* note 50, at 776-78.

53. *See id.* at 778 (explaining that the initial draft of the Clipper Chip allowed the seizure of electronic data by the government through back doors in computers thereby intruding on the private information encrypted by American citizens). Worse yet, the legislation encouraged the government to intrude on American citizens private information and communications by providing this back door. *Id.* The Fourth Amendment was designed to prevent such intrusive government conduct. *Id.* The 1995 redraft of the proposed Clipper Chip legislation allowed for third parties to hold the keys necessary for decryption. *Id.* at 778. Had it been passed, the redrafted version might have withstood Constitutional challenges, however it still implicated Fourth Amendment privacy concerns for both individuals and corporations. *Id.*

54. *See* Klopfenstein, *supra* note 50, at 780 (referencing the Arms Export Control Act, 22 U.S.C. § 2751 (1994); the International Trafficking in Arms Regulations, 22 C.F.R. § 120 (1998); the Export Administration Act, 50 U.S.C. app. § 2401 (1999); and the Export Administration Regulations, 15 C.F.R. § 730 (1998)).

55. *See* 47 U.S.C. § 1002(a)(3) (1999) (providing that a "telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.").

56. *See* Klopfenstein, *supra* note 50, at 780-83.

57. *See id.* at 779-80 n.108.

58. *See id.*

tions.[59] Therefore, a new means of handling the developing technology to strike a balance between both sides of the debate is warranted.[60]

2. *Proposed Legislation Regulating Encryption*

CESA is merely the most recent twist in the ongoing encryption debate between the government and privacy advocates.[61] CESA's initial draft eased the process by which law enforcement officials could obtain a sealed search warrant to enter a suspect's home or office to search a personal computer for incriminating evidence.[62] This search is performed by obtaining passwords and installing devices to override encryption, thereby revealing the plaintext.[63] The initial draft of CESA received a hostile response from the software industry, privacy advocates, and civil

---

59. *See id.*

60. See *Hack Attacks Raise Specter of Government Intervention*, 6 CDT POLICY POST No. 4 (last modified Feb. 16, 2000) <http://www.cdt.org/publications/pp_6.04.shtml>. The wake of attacks on e-commerce Web sites in early February, 2000, may serve as justification for legislation related to encryption and privacy in Cyberspace. *Id.* This legislation may place civil liberties and privacy rights in jeopardy by eroding advantages of anonymity in Internet communications and transactions. *Id. See also* Robert MacMillan, *Net Security Blankets Capitol Hill This Week*, NEWSBYTES NEWS NETWORK, Feb. 28, 2000 (explaining that a series of "denial of service attacks on popular World Wide Web sites" will encourage hearings and the introduction of CESA to Congress). CESA has faced strong opposition based on the argument that the nation's infrastructure should be advanced making encryption indispensable, rather than creating legislation that encourages government surveillance and monitoring. *Id.*

61. *See* Robert O'Harrow, Jr., *Justice Dept. Mulls Covert-Action Bill*, NEWSBYTES NEWS NETWORK, Aug. 20, 1999 (explaining that CESA follows previously unsuccessful efforts by the FBI and Justice Department officials attempting to secure back doors to computers and software allowing law enforcement officials to circumvent encryption). These proposals received little Congressional backing in the past. *Id.* Virginia Republican, Robert W. Goodlatte, the encryption advocate who sponsored the Security and Freedom Through Encryption Act ("SAFE"), explained that Congress desires to support legislation facilitating law enforcement's ability to handle the new technologies. *Id.* Congress wants to create a balance through such legislation that protects both the privacy rights of law-abiding citizens while providing law enforcement with the ability to handle encryption. *Id.* The need for a delicate balance of civil liberties and the ability for law enforcement officials to manage the problems concerning criminal use of encryption is essential. *Id.*

62. *See* Buzz Hunter, *e-Biz Buzz*, E-BUSINESS ADVISOR, Oct. 1, 1999 (surveying consumer frustration with Internet banking).

63. *See id.* at 2; *see also Web Right*; *Company and Business Marketing*, PC WEEK, Feb. 7, 2000, at 57 (explaining that the Clinton administration proposed CESA to extend the government's power of search by providing a means of counteracting encryption technology). CESA "would let government attorneys' seek to block disclosure of the means by which seized information was decrypted if the disclosure would 'compromise the techniques or mechanism for the purposes of future investigations.'" *Id.* The Clinton administration argues that current search powers are "wholly insufficient" when encryption is used to conceal the plaintext of data. *Id.*

libertarians,[64] while law enforcement officials supported it.[65] On September 16, 1999, the White House announced a revised version of CESA for Congressional consideration and speedy enactment.[66] The revised version eliminates some of the Fourth Amendment concerns regarding the process of obtaining encrypted data.[67] To effectively analyze CESA, it is necessary to understand how the history behind the value of privacy has influenced the Fourth Amendment.

D. The Value of Privacy and the Fourth Amendment

1. *The Value of Privacy in U.S. Society*

The American value of privacy is separate from the Fourth Amendment privacy right.[68] The legal principle of a right to privacy under the Fourth Amendment is preceded by the moral value of privacy that led to its conception.[69] Preceding the Fourth Amendment, Americans believed

64. *See Justice Dept. Seeks New Encryption-Related Authority*, *supra* note 30 (explaining that the proposed bill may violate Fourth Amendment rights by allowing officers to search a suspect's computer, alter a computer password, or decrypt encrypted information to obtain evidence). James Dempsey, counsel for the Center for Democracy & Technology, notes that CESA's initial draft would abolish free choice and shatter the Fourth Amendment right to privacy in one's own home. *Id.* In effect, CESA's states "[i]f you don't escrow your keys with a 3rd party where we can get them, we can come get them." *Id. But see* Hunter, *supra* note 62, at 2. Whereas CESA's goal is to provide law enforcement officials with the ability to inhibit criminal activity such as terrorism and child pornography, CESA could also be used in tax investigations to decrypt private information, a goal that is not stated in the enumerated policy of CESA. *Id.*

65. *See* Hunter, *supra* note 62 (noting that CESA increases law enforcement authority to manage the expanding use of encryption). Presently, law enforcement officials must obtain a search warrant providing access to a suspect's hard drive and the files contained within. *Id.* Encrypted files cannot be opened under current law or technology unless a key is provided. *Id.* CESA allows for the decoding of encrypted text either through access to a decryption key or through developing law enforcement technology. *Id.* "Courts could conceivably approve police entries into homes and offices to alter hardware or software," allowing plaintext files to be accessed and read. *Id.* Therefore, law enforcement officials would acquire expanded authority under CESA. *Id.*

66. *See generally* CESA, *supra* note 29.

67. *See* Jack McCarthy, *U.S. Relaxes Encryption Controls*, InfoWorld Daily News, Sept. 16, 1999 (noting that the Clinton Administration aimed for CESA to be in effect by Dec. 15, 1999 according to a White House statement).

68. *See* Vedder-Brown, *supra* note 40, at 1403-04 (explaining that "privacy" from a moral standpoint is different than the "right to privacy" protected under the Fourth Amendment).

69. *See* Ira Glasser, *The Struggle for a New Paradigm: Protecting Free Speech and Privacy in the Virtual World of Cyberspace*, 23 Nova L. Rev. 627, 627-28 (1999); *see also* Reilly, *supra* note 37, at *4-*6 (arguing that privacy should be viewed as a bedrock for American society, similar to the American values of life, liberty, and the pursuit of happiness). Privacy is fundamental to many aspects of daily life, including mental and physical health, religion, and lifestyle decisions. *Id.* at *8. However, cyberspace, and developing computer technology designed to simplify life actually increases the threat to privacy be-

a man's home was his castle, and any individual or government invading this home, without invitation, was trespassing.[70] In creating the Bill of Rights, our Founders debated the values that were crucial to preserve in drafting the governing law of this new land.[71] Privacy was a central concern of our Founders.[72] Before the American Revolution, British soldiers and customs agents entered the homes and offices of American colonists at will to conduct random searches.[73] The casualties of these searches were the American colonists.[74]

2. *The Fourth Amendment Right to Privacy*

Our Founders believed that privacy in the form of freedom from discretionary government searches,[75] especially in one's own home, was necessary for liberty to endure.[76] The Fourth Amendment was drafted to protect this value of privacy against government intrusion.[77] The right to privacy that the Fourth Amendment protects is "the right most valued by civilized people."[78] The right to privacy is the foundation for many other rights.[79] If Fourth Amendment rights are weakened through legislation responding to new technology, other rights will ultimately disintegrate, causing the foundation of America to slowly vanish.[80] Initially, the Fourth Amendment acted as a legal barrier protecting the four walls of an individual's home or business and all that occurred inside.[81] As technology evolves and new privacy issues emerge, so must the law continue to evolve to encompass those issues. The computer has transformed society,[82] and thus, the law.[83] Case law has expanded the

---

cause it requires new laws and confounds the legal analysis of existing privacy interpretations. *Id.* at *6.

70. *See* Glasser, *supra* note 69, at 627-28 n.1 (noting that America's Founders did not recognize that a woman's home was likely her castle also).

71. *See id.* at 628.

72. *See id.* at 638.

73. *See id.*

74. *See id.*

75. *See* Glasser, *supra* note 69, at 638.

76. *See id.*

77. *See id.* (articulating the post revolution demand for security and freedom from government intrusion).

78. Hunter, *supra* note 51, at 197 (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).

79. *See id.* at 197 (explaining that the right to be let alone is the "one theme that pervades the entire constitutional structure.").

80. *See id.* at 199.

81. *See id.*

82. *See* David C. Tunick, *Has The Computer Changed The Law?*, 13 J. MARSHALL J. COMPUTER & INFO. L. 43 (1994). "Computers are with us everywhere: medicine, business, transportation, banking, shopping, entertainment, travel, education, and more." *Id.* "They are entwined in many aspects of our lives." *Id.*

scope of individual privacy rights under the Fourth Amendment.[84] CESA may impact the way courts view electronic communications and information in light of Fourth Amendment privacy rights.[85] Therefore, an analysis of the Court's response to previous technology in light of the Fourth Amendment is necessary to provide a foundation for understanding the impact CESA may have on the Fourth Amendment.

3. *Technology's Effect on Fourth Amendment Has Prompted Litigation*

The right to privacy is not expressly guaranteed in the United States Constitution. However, the Supreme Court has interpreted the Fourth Amendment to provide individuals with the right to be free from government intrusion.[86] Because no explicit right to privacy is guaranteed, individual privacy has broadly been interpreted. However, an implicit right to privacy is clear in the Fourth Amendment's prohibition of unreasonable government searches and seizures.[87]

While early telephone conversations were private, the advent of wiretapping allowed the government to act as a fly on the wall of an individual's home listening to what was previously a private telephone con-

---

83. *See id.* Computers have become involved with many areas of the law including the way courts interpret existing law in light of new technology. *Id.*

84. *See* Glasser, *supra* note 69, at 637-38 (explaining how the invention of the telephone has affected Americans by transforming the rights that the Fourth Amendment was designed to protect). *See also* Lillian R. BeVier, *The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break Up of AT&T*, 51 STAN. L. REV. 1049, 1061-62 (1999) (noting reasons for the difficulty of enacting legislation relating to technology). "[E]nacting legal solutions to complex problems of any kind is always politically difficult and time consuming . . . correcting legislatively enacted policy mistakes is often an onerous political chore." *Id.* The breadth of changing technology intensifies the inadequacies of proposed legal solutions. *Id.* For example, the development of encryption has exacerbated legislative attempts to regulate privacy in Cyberspace.

85. *See* John T. Soma & Charles P. Henderson, *Encryption, Key Recovery, and Commercial Trade Secret Assets: A Proposed Legislative Model*, 25 RUTGERS COMPUTER & TECH L.J. 97, 122 (1999) (explaining that the computer industry, business community and privacy groups argue that "law and tradition do not require private citizens to take positive action to assist the government in surveilling them."). The government should not require American citizens to provide the government with access to personal assets, communications, diaries, financial records, or personal data. *Id.* Encryption, and the right and value of privacy that is protected by encryption outweighs the harm done in the few instances where encryption hampers law enforcement. *Id.* Encryption is designed to protect privacy, and widespread use of encryption can prevent crime. *Id. See also* Security and Freedom Through Encryption (SAFE) Act, H.R. REP. No. 105-108, at 6 (1997).

86. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (describing the "zones" of privacy created by the Bill of Rights). *See also* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1345 (1992) (providing a comprehensive history of the development of privacy rights under the Fourth Amendment).

87. *See* Fred H. Cate, *Privacy and Telecommunications*, 33 WAKE FOREST L. REV. 1, 21 (1998).

versation.[88] As with any existing law applied to new technology, litigation ensued. The first constitutional challenge to wiretapping was raised in *Olmstead v. United States*.[89] The defendant, a suspected bootlegger, was convicted based on wiretap evidence.[90] Olmstead was convicted against his argument that the wiretap search violated his Fourth Amendment rights since there was no warrant or probable cause.[91] The case was narrowly decided, and the majority held that the federal government had the authority to wiretap without need for a warrant under the Fourth Amendment since physical intrusion of the premises did not occur.[92] In the *Olmstead* dissent, Justice Brandeis argued that wiretaps were subject to the Fourth Amendment, required a warrant, and inevitably should be prohibited.[93] Brandeis compared wiretapping one's telephone line to opening up a sealed letter and invading the privacy of the both the person calling and the suspect.[94] Brandeis' argument foreshadowed today's conflicts between modern technology and the Fourth Amendment.[95]

Olmstead was overruled in a similar case, *Katz v. United States*, where the court held that warrants are required before wiretaps can be authorized and may only be issued on a showing of probable cause.[96] In *Katz*, the majority embraced Justice Brandeis' *Olmstead* dissent, and the concept of privacy implicit in the Fourth Amendment was specifically recognized for the first time.[97] Justice Harlan's concurring opinion set forth the "reasonable expectation of privacy" test that was later adopted in *Terry v. Ohio*.[98] In 1977, the Supreme Court decided *Whalen v. Roe*

88. *See* Glasser, *supra* note 69, at 639.

89. Olmstead v. U.S., 277 U.S. 438 (1928).

90. *See id.* at 456.

91. *See id.* at 456-58.

92. *See id.* at 465-66 Since the wiretap did not invade Olmstead's home, it was not a physical trespass in violation of the Fourth Amendment. *Id.*

93. *See id.* at 475-76 (Brandeis, J., dissenting).

94. *See Olmstead*, 277 U.S. at 476.

95. *See id.* at 474 (warning against the "progress of science [providing] the Government with means of espionage" essentially unrestricted by the Fourth Amendment). Brandeis argued that unreasonable searches and seizures under the Fourth Amendment must also apply to new technologies including wiretaps. *Id.* By requiring a physical trespass to invoke an individual's right to Fourth Amendment protection, developing technologies will lack protection from unreasonable government intrusion. *Id.* at 471-74. The holding in *Olmstead* in conjunction with developing technologies provided the government with a subtler, yet more sweeping means of invading individual privacy. *Id.* at 473.

96. Katz v. U.S., 389 U.S. 347, 357-58 (1967).

97. *Id.* at 351-52 (quoting J. Stewart, who explained that what an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

98. *Id.* at 360-61 (Harlan, J., concurring) (providing the first glimpse at the "reasonable expectation of privacy" test that was later adopted by the majority). *See also* United States v. Simons, 29 F. Supp.2d 324, 326-27 (E.D. Va. 1998) (citing Katz v. United States,

first recognized an individual's right to keep personal information private and prevent unwarranted government disclosure of personal information.[99]

Congress then passed legislation allowing law enforcement officials to conduct wiretaps upon court order[100] requiring an accounting of the results.[101] The results of this accounting are staggering and clearly show that the Fourth Amendment's narrowly targeted search warrant requirement is not being obeyed. Otherwise, warrants issued on law-abiding citizens would be minimized.[102] To prevent similar results, an

---

389 U.S. at 361 (Harlan, J., concurring)) (explaining the two prongs of the reasonable expectation of privacy test). The first prong is subjective since it requires that "[t]he person must have had an actual or subjective expectation of privacy." *Id.* The second prong objectively requires that this subjective expectation of privacy is one that society will recognize as 'reasonable.'" *Id.* *See also* Terry v. Ohio, 392 U.S. 1, 31 (1968) (Harlan, J., concurring) (establishing the sliding scale of intrusiveness where the more intrusive the search, the more demanding that procedural requirements are present establishing the search's reasonableness). *Id.* at 31. The majority in Terry adopted Justice Harlan's "reasonable expectation of privacy" test set forth in his Katz concurrence. *Id.* at 9. The majority expands on this "reasonable expectation of privacy" test by explaining that "there is no ready test for determining reasonableness." *Id.* at 21 (quoting Camara v. Municipal Court of City and County of San Francisco, 387 U.S. 523, 536-37 (1967)). However, where an individual may have a "reasonable expectation of privacy," he is protected against unreasonable government intrusion. *Id.* at 9. "'No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law.'" *Id.* (quoting Union Pac. R. Co. v. Botsford, 141 U.S. 250, 251 (1891)). *See also* COMPUTER SEARCH & SEIZURE WORKING GROUP, U.S. DEP'T OF JUSTICE, FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 17 (1994) (explaining that the government must be a state actor to trigger Fourth Amendment protections). *See also* WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.6, at 70 (3d ed. Supp. 1999) (explaining that continuously evolving technology will force the "reasonable expectation of privacy" test to evolve with society's rapidly changing expectations of reasonableness). *See generally Katz*, 389 U.S. 347 (Harlan, J., concurring). If either of the two prongs is not met, the government may search and seize without the prerequisite of a warrant and without showing reasonable suspicion. *Id.* The test is flexible since it changes along with society's current expectations of reasonableness. *Id.*

99. *See* Whalen v. Roe, 429 U.S. 589, 598-600 (1977) (holding that a state statute requiring physicians to submit copies of prescriptions for abused drugs for a state computer file was a reasonable exercise of police power since the government had a "vital interest" in controlling the distribution of dangerous drugs); *cf.* Florida v. White 526 U.S. 559 (1999) (holding that a warrantless search and seizure was reasonable under exigent circumstances). *See generally* Griffin v. Wisconsin, 483 U.S. 868, 877-880 (1987). Exigent circumstances exist where law enforcements officials have "special needs" rendering a warrant and probable cause requirements impracticable. *Id.*

100. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 236 (codified as amended at 18 U.S.C. § 2518 (1994)).

101. *See* 18 U.S.C. § 2519 (1994).

102. *See* Ira Glasser & Herman Schwartz, *Your Phone is a Party Line*, HARPER'S MAG., Oct. 1972, at 108 (reporting that when federal eavesdropping did not exist but state eavesdropping did, state officials listened to 66,716 conversations without a single reported con-

examination of CESA's policy and a sectional analysis is necessary to determine whether its implementation will cause the government to overstep its bounds and take on the role of Big Brother.

III. ANALYSIS

A. THE POLICY AND SECTIONAL ANALYSIS OF CESA

1. *The Policy Justifying CESA*

American history is replete with complex social, technological, and economic forces creating opportunity and promise.[103] America's rapid development created challenges for the government,[104] and in turn, the American people.[105] World War II created a new global economy and set the stage for America to enter the Information Age.[106] As the evolution

---

viction). This number increased when federal officials eavesdropped. *Id.* In 1970 and 1971, 870,190 conversations were overheard by the federal government, none of which involved a homicide or kidnapping. *Id.* at 111. In 1971, ninety percent of convictions were for gambling, six percent were drug crimes, and four percent were other offenses. *Id. See also* Glasser, *supra* note 69, at 643-44 (providing 1996 statistics). Two point two million conversations were wiretapped, 1.7 million of which prosecutors found not to be incriminating. *Id.* None of the wiretap orders were issued for arson, explosives, or weapons investigations. *Id. See also Wiretapping*, ELECTRONIC PRIVACY INFORMATION CENTER WIRETAP PAGES (last modified Jan. 20, 2000) <http://www.epic.org/privacy/ wiretap/> (noting the increase in requests for wiretaps in 1998 according to a report by the U.S. Courts). The report noted that in 1998, only two wiretap requests were denied at the State and Federal levels. *Id.* Moreover, electronic surveillance requests increased by 12 percent overall in 1998. *Id.* In comparison, wiretaps increased only three percent in 1997, and the Administrative Office of U.S. Courts' 1997 report notes that of all of these wiretaps in 1997, only two were computer related. *Id.* The fact that only two of all 1997 wiretap requests were computer related appears to justify law enforcement's need to access encrypted information and allocate resources to develop a means of decryption at the cost of individual's privacy.

103. *See The Clinton Administration's White Paper*, *supra* note 27, § 1 (noting that Congress and the Administration have been working on creating an infrastructure for a new society since the Louisiana Purchase). Between the 1820's and 1900, American railroads expanded the possibilities for travel and opened up our developing nation by laying more than 2,000 miles of track each year, on average. *Id.* § 1. Technology continued to evolve in America through the Industrial Age where machinery and assembly lines allowed for mass production. *Id.* Ford's mass production of the Model T and the first air flight by the Wright brothers brought new means of travel to America making expansion and further technological developments increasingly possible. *Id.* The telephone revolutionized communication making it possible for news and information to travel across America instantaneously. *Id.* The American economy began to change from agrarian to industrial, thereby allowing for economic opportunity based on innovation rather than heritage creating. *Id.*

104. *See id.*

105. *See id.* The Great Depression slowed the rate of economic development in America. *Id.* The government responded by creating new programs aimed at restoring productivity while recognizing technology as necessary to guiding America through the struggles of the Depression. *Id.*

106. *See id.* Following World War II, a global economy began to emerge through the development of science and technology in the U.S. *Id.* During this time, the development

of technology has empowered industry to collect, utilize and transfer large amounts of data, it has also presented new legal challenges.[107] In the age of Cyber America, our nation faces the challenge of maintaining order in a globally linked society[108] while affording individuals personal privacy through technology such as encryption.[109] Encryption is the primary concern of CESA.

While government policy supports law enforcement's need to decrypt data in the interest of national security,[110] the policy also supports the need for encryption to protect America's economic infrastructure.[111]

---

of computers rapidly expanded the importance of the field of technology. *Id.* Computers have now become essential in the operation of all businesses both for transmission of information and data storage. *Id.* § 2.

107. *See id.* As a result of the pervasiveness of computer technology and the changes it effected in the way people communicate, America's legal system has been compelled to respond to technology. *Id.*

108. *See id.* A society dependent on computer communication is both promising and a danger to national security. *Id.* Balancing the risks and benefits of developing computer communication technology is essential to advancing national interests. *Id.* Computers are driving the American economy, recreation, and education. *Id.* The industry in the U.S. is changing from a nation of people who simply produce things to a nation of "knowledge workers" relying on the engine of computers to pull the productivity train. *Id.* Pressed for time and in search of speed, computers have responded to the demands of "knowledge workers." *Id.* From barcodes on grocery items, to clothing, books, airline reservations, and Internet services, face-to-face communication and customer service is decreasing while computer communication, contracts, and commerce increases. *Id.* Businesses rely on computer networks and the World Wide Web to exchange training, network suppliers, and increase productivity. *Id.* Educational institutions rely on the Internet to conduct research and communicate with students and other institutions. *Id.* The fields of science and medicine transmit data electronically to other professionals around the world. *Id.* The world is rapidly growing smaller through the elimination of traditional time and place boundaries in favor of "cyberspace." *Id.*

109. *See The Clinton Administration's White Paper, supra* note 27, § 2 (explaining that the law must respond to the evils inherent in any new technology). "The danger posed by evil individuals using these powerful new tools grows by the day." *Id.* "Just as other technologies have the risk of being abused, it is necessary" for the government to respond through preventative measures attempting to ensure U.S. safety. *Id.*

110. *See* Glasser, *supra* note 69, at 627-28 (noting that computer technology, specifically encryption, is being exploited by those who "prey on the innocent" by masking criminal activity).

111. *See The Clinton Administration's White Paper, supra* note 27, § 2. Hackers destroy "cyber-property," maliciously manipulate private information, and crooks break into corporate computers "either stealing funds directly or extorting payments from companies anxious to avoid more expensive disruption." *Id.* If this information is so readily available to criminals wishing to exploit it, and hackers can so easily break the barrier of businesses disrupting our economy, this behavior must be stopped. *Id.* The next step is to examine how to stop this behavior, with the answer being stronger encryption. The government argues, however, that to stop crime, access to tools for decrypting encrypted data is essential. *Id.* § 4. *See generally* CESA, *supra* note 29 (detailing how the government is attempting to regulate encrypted data through CESA). However, it is illogical to believe that

Through CESA, the government attempts to address the encryption challenge by counterbalancing law enforcement's need to protect national security with the desire to promote economic growth.[112] CESA provides law enforcement officials with the authority to obtain the plaintext of encrypted data through access to decryption keys and by establishing a Justice Department-operated center aimed at developing decryption technology when a key is not stored.[113]

CESA's policy is similar to the Clinton Administration's Clipper Chip proposals. The Clipper Chip, like CESA, was proposed to promote telecommunications security, national security, and public safety.[114] While encouraging the use of encryption technology, the Clipper Chip would have allowed government officials to intercept encrypted commu-

---

providing the authority and ability to decrypt data through access to decryption keys will prevent criminal activity.

112. *See The Clinton Administration's White Paper*, *supra* note 27, § 4 (noting that CESA is the proposed new paradigm attempting to strike this balance). The legislation must provide new tools for "information security and privacy . . . and updated tools for law enforcement." *Id.* *See also* Robert MacMillan, *Hatch Won't Hatch Clinton Net Security Idea*, NEWSBYTES NEWS NETWORK, Mar. 3, 2000, at 1 (explaining that CESA is a roadmap of do's and do not's that government agencies and law enforcement officials must obey when investigating and prosecuting encryption cases).

113. *See* Robert MacMillan, *SAFE Encryption Act Seems Safely Stuck In House*, NEWSBYTES NEWS NETWORK, Oct. 6, 1999, at 2; *cf.* James D. Polley, IV, *Capital Perspective*, PROSECUTOR, Nov./Dec. 1999 (explaining that the FBI will revive authorization for their technology center to develop a means for decrypting encrypted data, and $80 million to execute its task). Although not a provision of CESA, the Clinton administration intends to allocate $500 million to enhance information security at the Defense Department. *Id.* at 18. *See also* MacMillan, *supra* note 112, at 1 (explaining CESA's proposed allocation of $80 million to the FBI to develop a means of decrypting encrypted information). *See also* David M. Nadler & Valerie M. Furman, *Administration Relaxes Restrictions On Encryption Software*, 17 ANDREWS COMPUTER & ONLINE INDUS. LITIG. REP. 3, Nov. 2, 1999 (explaining that in addition to CESA's allocation of $80 million to the FBI, $500 million will be given to the Defense Department to enhance its information security).

114. *See* William A. Hodkowski, Comment, *The Future Of Internet Security: How New Technologies Will Shape the Internet and Affect The Law*, 13 SANTA CLARA COMPUTER & HIGH TECH L.J. 217, 243 (1997) (noting that the Clinton Administration aimed to promote security objectives by mandating the use of the proposed Clipper Chip in all secure communications equipment sold to the government). The key escrow technology used in the Clipper Chip is distinguishable from CESA's encryption proposal. *Id.* The Clipper Chip required installation inside the computer whereas CESA regulates decryption keys through legislation imposing criminal penalties. *Id.* The Clipper Chip and CESA are similar in that both policies aim to correct the same concerns. *Id.* Both attempt to promote national security by attempting to prevent U.S. infrastructure attack and provide public safety by implementing a means to decrypt encrypted information about, or used to facilitate, criminal activity. *Id.* Both the Clipper Chip and CESA aim to provide telecommunications security through encryption technology, provided that the government has a means of decrypting the information. *Id.* The government maintains through both proposals that they "do not want to deny Americans the right to strong cryptography," however, government wants access to the plaintext of encrypted data in the interests of society. *Id.* at 244.

nications through a unique key providing a back door into computers through their communication devices.[115] An outcry of civil libertarians and images of Big Brother trampling on the privacy rights and values of law-abiding citizens caused the Clipper Chip proposal to fail.[116] With the same policy aims, CESA may face similar challenges.[117] Unfortunately, the government will likely prevail in the war against encryption, and challenges to CESA will likely be a losing battle.[118] The cost of this battle will be the security of information and privacy of law-abiding American citizens.

2. *CESA's Text Falls Short of Promoting the Security of Information and Privacy*

CESA aims at promoting the security of information and privacy.[119] The government claims that CESA creates protections for persons and businesses storing decryption keys with recovery agents.[120] Although

115. *See id.* at 244 (explaining the key escrow technology implemented by the Clipper Chip). The Clipper Chip method allows "all communications encrypted with the chip, regardless of what session key is used or how it is selected, to be decrypted through a special key unique to that particular Clipper Chip and a special Law Enforcement Access Field (LEAF) transmitted with the encrypted communications." *Id.*; *see also* Doug Brown & L. Scott Tillett, *Bill Reopens Encryption Access Debate,* FEDERAL COMPUTER WEEK, Aug. 16, 1999, *available at* <http://www.fcw.com/pubs/fcw /1999/0816 /fcw-newsencrypt-08-16-99.html> (noting that the Clipper Chip was designed to "protect private communications" while providing a "'backdoor' for law enforcement officials to decrypt necessary data.").

116. *See* Hodkowski, *supra* note 114, at 243 (explaining that if the Clipper Chip had passed, it would have been the first step in the U.S. government's ability to mandate key escrow encryption in all Cyberspace communications, computerized data, and information). It is unclear whether commercial and private encryption users have the Fourth Amendment right to resist mandatory key escrow because the courts place great importance on both sides of the debate, civil rights, and national security and law enforcement. *Id.* Case law has not yet examined the issue of whether civil rights or national security and the needs and rights of law enforcement will win out in this conflict. *Id.*; *see also* Brown & Tillett, *supra* note 115 (noting that the Clipper Chip initiative ceased after outcry by privacy groups). Further, the computer industry warned that the initiative could facilitate potential abuse of power by law enforcement agencies. *Id.*

117. *See* Reilly, *supra* note 37, at 28 (explaining that "[e]rror in legislation is common, and never more so than when technology is galloping forward."). The galloping horse causing error in privacy legislation is Cyberspace. *Id.*

118. *See* Polley, *supra* note 113 (explaining that support for the lifting of encryption limits, the technology industry's financial power, and political power advanced by technology interests, makes the passage of CESA inevitable).

119. *See* Letter from Jon P. Jennings, Acting Assistant Attorney General, *Office of the Attorney General,* to the Honorable J. Dennis Hastert, Speaker, *U.S. House of Representatives* at 2 (Aug. 5, 1999), *available at* (visited Oct. 7, 1999) <wysiwyg://26/http://www.cdt.org/crypto/CESA>.

120. *See id.* (explaining that the security of encryption systems depend on "the security of the keys that can be used to decrypt data."). Jennings explains that "clear procedures are needed to ensure that these keys are protected by 'recovery agents' in the business of

the government argues that keys in the hands of any third party require protection, access to these keys is provided under a statutory standard[121] not found in any other statute and unsupported by judicial precedent.[122]

Keys stored with third parties are entitled to protection under CESA.[123] However, these keys are not constitutionally protected under the Fourth Amendment once obtained by third parties; thus, neither is the encrypted information.[124] Further, Fourth Amendment privacy protections[125] for information stored on networks are not established by CESA.[126] By concentrating on the trees through its narrow focus on access to keys and passwords, CESA ignores the forest of information and documents stored on networks.[127] An act truly protecting electronic security in cyberspace would establish network regulations and define the scope of protection under the act.[128]

Rather than mandating probable cause to seize keys, CESA creates a new standard,[129] declaring that there is "no constitutional privacy in-

---

storing keys on behalf of others." *Id.* "Clear procedures are also needed regarding the law enforcement agencies that may obtain decryption keys pursuant to lawful authority to investigate criminal activity." *Id.* CESA creates protections such as prohibiting disclosure of information by recovery agents and prohibiting decryption of data without notice to the person storing the key or obtaining a court order. *Id.* CESA also prohibits recovery agents from selling or disclosing customer lists to other parties. *Id.*

121. *See* Appendix I (detailing the pertinent portion of CESA relating to recovery information by amending chapter 121 of Title 18 of the United States Code).

122. *See Initial CDT Analysis of the Clinton Administration's Proposed Cyberspace Electronic Security Act (CESA): Standards for Government Access to Decryption Keys* [hereinafter *Initial CDT Analysis*] (Sept. 23, 1999) <http://www.cdt.org/crypto/CESA/CESA> (analyzing the portion of CESA aimed at protecting stored information while contemporaneously providing government access to decryption keys). Law enforcement officials can access decryption information held by third parties under CESA's unique statutory standard. *Id.* The court order specified in subsection (b)(1) and (4) sets forth this unique standard. *Id.* The CESA standard requires that a magistrate or trial court judge determine whether there is a "constitutionally protected privacy interest in certain plaintext" based on the government's presentation of evidence without challenge by the alleged offender. *Id.* Any statutory privacy interest in the plaintext is irrelevant. *Id.* The problem with this standard is that it is inferior to the Constitution's requirement for government access to decryption keys, which is "probable cause to believe that a crime is being committed and notice at the time of the seizure." *Id.*

123. *See id.*

124. *See id.*

125. *See id.* at 5.

126. *See id.* at 4-5 (explaining that protections exist only in the "remote computing provision found in 18 U.S.C.§ 2703(b) which provides less than Fourth Amendment protection.").

127. *See Initial CDT Analysis, supra* note 122, at 1.

128. *See id.* at 4-5.

129. *See id.*

terest in the plaintext" of data.[130] CESA allows the government to seize the plaintext information of encrypted data and the decryption key from a third party recovery agent under a single warrant.[131] Although two distinct steps are necessary to obtain encrypted information if a decryption key is stored with a third party, only one warrant is required under CESA.[132] Two warrants should be required: one to seize the decryption key from a third party recovery agent, and a second warrant to search the computer and seize the data or communications. Certainly, CESA's unique standard does not conform to the standards established for the Fourth Amendment.[133]

Traditionally, the Fourth Amendment protects information stored on a home or office computer. For any information to be seized from a person's computer, it shall be required that a warrant be issued. The issuance of this warrant is based upon a showing of probable cause indicating that the evidence sought is likely to include evidence of a prior or ongoing crime.[134] Courts have held that when information is given to a third party it is no longer private and, thus, constitutional privacy rights associated with this information are lost.[135] It is unclear whether stored decryption keys cause the loss of privacy rights in information, or rather, provide for constitutional privacy protections because the information is intended to remain private.[136] CESA's statutory standard extends only

130. *See id.*

131. *See id.*

132. *See id.*

133. *See* U.S. CONST. amend. IV (providing for the issuance of a warrant on based on "probable cause . . . and particularly describing the place to be searched and the persons or things to be seized."). The place to be searched and item to be seized from a key recovery agent is the key from the location of the recovery agent. *Id.* The plaintext information to be seized and computer holding this information is entirely distinct from the former. *Id.* It would defy the Fourth Amendment to find that one warrant is sufficient to obtain both a decryption key from a recovery agent and the plaintext of encrypted data from an individual's computer because law enforcement officials must take two very separate steps to achieve the desired result. *Id.*

134. *See Initial CDT Analysis, supra* note 122, at 2.

135. *See id.*

136. *See id.* (noting that when privacy status of e-mail and cellular phone conversations were questionable, Congress created the Electronic Communications Privacy Act of 1986 ("ECPA") which protected privacy rights by requiring probable cause to access this information). While the courts have not yet considered whether keys in possession of third parties are protected under the Fourth Amendment, CESA clearly states that they are not. *Id.* at 3. A narrow privacy right is provided by CESA to protect escrowed keys from other parties, yet the government is provided with access based on a standard falling short of the Fourth Amendment. *Id.* CESA clearly states that there is "no constitutionally protected expectation of privacy in recovery information held by a third party . . . ." *Id.* No court has held on the issue of whether decryption keys stored with third parties are Constitutionally protected; CESA states that they are not, but has not been passed yet. *Id.* Therefore, this

to constitutionally protected privacy rights,[137] information carrying with it a "reasonable expectation of privacy."[138] Whether CESA extends to statutorily protected privacy rights is unclear.[139] The discussion of CESA's ambiguity accompanies the analysis of the legal concerns regarding CESA's effectiveness.

An individual who chooses to encrypt information intends for that information to remain private. To protect this privacy, despite CESA's unique standard,[140] CESA should require stricter warrant authorization procedures.[141] CESA should be required to follow federal wiretap warrant authorization guidelines mandating that states abide by the requirements of Title III and the Electronic Communications Privacy Act ("ECPA").[142] A federal wiretap warrant requires an application satisfy-

---

issue remains unresolved. *Id.* Should CESA become law, this issue would likely be resolved in defeat of privacy rights.

137. *See supra* note 116 and accompanying text.

138. *Initial CDT Analysis, supra* note 122, at 3 (explaining the constitutional standard for privacy of information); *see also* Berman & Mulligan, *supra* note 37, at 567 (explaining that privacy protections existed for items when they were in ones home, but now, when personal thoughts or communications, such as a diary, is moved onto a computer instead of being stored "under the bed" the Fourth Amendment no longer affords them protection). In an age where computers are used for everything including grocery shopping, storing financial records, holding medical information, and communicating with one and other, what was once protected if within the walls of our homes should not desist Fourth Amendment protection simply because times have changed and these items have been placed on a computer. *Id. See also* U.S. v. Morgan, 744 F.2d 1215 (6th Cir. 1985); *see also* U.S. v. Turner, 528 F.2d 143 (9th Cir. 1975); *see also* U.S. v. Simpson, 944 F. Sup. 1396, 1403 (S.D. Ind. 1996). There is, however, no reasonable expectation of privacy in contraband. *Id. See also* U.S. v. Place, 402 U.S. 696 (1983). The governmental intrusion infringes upon personal and societal values only when the acts protected are within the law. *Id.*

139. *See id.* at 3 (explaining that statutorily protected privacy rights may become nonexistent if CESA is passed). One such example is that while the ECPA protects privacy in e-mail, it is unclear whether there is a "reasonable expectation of privacy" with regard to e-mail. *Id.* Conflict could arise through CESA rendering what is statutorily protected as unprotected under CESA's "constitutionally protected" standard. *Id.*

140. *See id.* at 5 (detailing CESA's statutory standard that is unsupported by judicial precedent). This standard falls short of the Constitution's requirement that probable cause exists demonstrating that a crime is being committed, and a warrant or warrant exception is present. *Id.* This standard is inadequate, since notice is not provided to the alleged offender at the time of the seizure. *Id.* CESA's unique notice standard is Constitutionally inadequate because it requires a trial court judge or magistrate's determination of whether there is a "constitutionally protected privacy interest in certain plaintext" without attention to whether a statutory privacy interest in the plaintext. *Id.* This determination is made in an *ex parte* proceeding based on the merits of the government's unchallenged presentation of evidence. *Id.*

141. *See id.*

142. Anjali Singhal, *The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography*, 7 STAN. L. & POL'Y REV. 189, 192 (1996) (explaining that the Title III and ECPA requirements are minimal, and further protection against abuse may be ascertained by stricter state laws).

ing the ECPA requirements that mandate disclosure of specified details relating to the potential wiretap.[143] This application must be reviewed by a Judge of competent jurisdiction who determines whether probable cause is present.[144] If the judge approves the application and issues a warrant,[145] the law enforcement official may then conduct the wiretap in good faith.[146] Title III and the ECPA have been interpreted in light of federal wiretaps to prevent law enforcement officials from retaining

143. *See id.*

144. *See id.* at 192-93. A judge must remain neutral and detached when reviewing a wiretap application because the judge has "great latitude in determining whether or not probable cause exists."

145. *See id.* at 200 n.55. *See also* United States v. Upham, 168 F.3d 532 (1st Cir. 1999), *cert denied* 119 S. Ct. 2353 (1999) (explaining that a warrant must contain a particularized description of the place to be searched, things to be seized, and must be supported by probable cause in order to limit the law enforcement official's discretion in determining what is seized). The required specificity of the warrant is determined by the facts of the case and the items involved. *Id. See also* United States v. Loy, 191 F.3d 360 (3d. Cir. 1999). When a warrant includes a description allowing for the seizure of items that should not be seized, then the warrant is overbroad. *Id.* Warrant exceptions do not always apply in computer evidence situations. *See* generally United States v. Lattimore, 87 F.3d 647 (4th Cir. 1996). A party may consent to the search of their computer and the evidence may be admissible if the consent was voluntary, however, the totality of the circumstances must be examined. *Id.* The accused's knowledge of the right to refuse consent is one factor to be examined in determining whether the suspect's consent was voluntary. *Id.* If consent is given but part of the computer or information is encrypted, the search is generally limited to the portion of the computer or information that does not contain encrypted information. *Id. See generally* Untied States v. Hotal, 143 F.3d 1223 (9th Cir. 1998). If the entry into the place where the computer is stored is illegal, then the evidence found therein is tainted although a warrant for the information or computer was valid. *Id. See also* United States v. Turner, 169 F.3d 84 (1st Cir. 1999) (explaining that the scope of consent provided must be the determinative factor limiting the scope of the search).

146. *See* U.S. v. Leon, 468 U.S. 897, 914 (1984) (requiring objective reasonableness in deciding whether a law enforcement officer used good faith in carrying out a search warrant). If the officer objectively used good faith in carrying out a search warrant but the warrant was not supported by probable cause, or the officer acted in good faith without a warrant because he believed probable cause was present, the fruits of the search will likely not be suppressed. *Id.* at 914-15. A problem may arise concerning a search warrant for encrypted data, however, if the officer cannot act in good faith due to a lack of technical knowledge relating to encryption. Further, a lack of technical knowledge may be problematic because the scope of a warrant may be too broad and lack specificity in describing the encrypted items to be seized. If the Magistrate signing the search warrant lacks sufficient technological knowledge to fully understand the scope of the search, then a warrant may be improperly issued. Educating officers, prosecutors, and judges about our rapidly developing technology is essential to providing the justice guaranteed under the Fourth Amendment. Continuing education will prevent encryption technology premised search warrants from being "rubber stamped" and promote fairness to the suspected individual. Continuing education in the area of search warrants for technological advances could decrease the litigation of such Fourth Amendment issues, thereby promoting judicial economy. *See generally* Hallinan v. Mitchell, 418 F. Supp. 1056 (N.D. Cal. 1976).

broad powers at the cost of privacy.[147] If CESA incorporates these provisions and strict regulations, privacy protections will increase and civil libertarians' fears may dissipate.

3. *CESA's Delayed Notice Provision Prevents Individuals from Protecting Their Own Interests*

CESA allows delayed notice of 90 days, and potentially indefinitely, upon a showing of good cause.[148] The alleged offender receives no opportunity to protect his own interests.[149] The government argues that contemporaneous notice could be detrimental to an investigation.[150] However, if the encrypted records are stored, delayed notice is unnecessary since notice can be provided contemporaneously with the seizure of keys from any third party recovery agent.[151] While delayed notice may be helpful in intercepting and secretly decrypting encrypted communications, it is unlikely that individuals encrypting criminal communications will escrow decryption keys, providing accessibility to incriminating information.[152] Furthermore, the delayed notice provision places an individual's Sixth Amendment right "to be informed of the nature and cause of the accusations" in jeopardy.[153] The Sixth Amendment gives an indi-

147. *See* Singhal, *supra* note 142, at 193; 18 U.S.C. §§ 2510-2521, 2701-2709 ("ECPA") (1994 & Supp. III 1997) (protecting private electronic communications from interception and disclosure by the government while in transit). The ECPA generally requires the government to obtain a court order before searching electronic information or communications. *Id.* Exceptions to this general rule do apply, however. *Id.* For example, only party in an electronic communication must consent to disclosure. *Id.*

148. *See* CESA, *supra* note 29, § 203 (amending Title 18 § 2714 of the United States Code by adding the following provision regarding notice).

> § 2714. Notice of access to recovery information held by third parties and obtained by a governmental entity. A governmental entity that has knowingly obtained recovery information by compulsory process other than under section 2712 of this title, shall, if such recovery information is held by the compelled party on behalf of another person or entity, notify such person or entity, if known, that the recovery information was obtained. Such notice shall be provided within 90 days of the date on which the government obtains the recovery information, and shall state the date on which the recovery information was disclosed. On the government's ex-parte showing of good cause, a court of competent jurisdiction may postpone the giving of notice. Notice under this section shall be provided by personal service, or by delivery by registered or first-class mail.

Id.

149. *See id.*

150. *See Analysis The Cyberspace Electronic Security Act of 1999* (Sept. 13, 1999) (visited Sept. 17, 1999) <wysiwyg://20/http://www.cdt.org/CESA/CESArevfactsheetanalsys.shtml> (providing the government's analysis of CESA which explains that delayed notice is available for good cause, but does not specifically detail what constitutes good cause).

151. *See id.; see also Initial CDT Analysis, supra* note 122.

152. *See id.*

153. *Web Rights; Company Business and Marketing, supra* note 63, at 57.

vidual accused of a crime the right to establish a defense against the accusation through notification of the "nature and cause of the accusation."[154] CESA's delayed notice provision does not provide this Sixth Amendment right since the delayed notice provision does not accommodate the alleged offender's right to protect his own interests.

Rather than allowing CESA's balance to tip in favor of law enforcement's need to decrypt encrypted text, CESA should provide alleged offenders with the opportunity to challenge the decryption of encrypted information. If a warrant requirement similar to that of wiretapping is imposed, the alleged offender receives contemporaneous notice that a key was seized and that information will be decrypted. The offender would not have the opportunity to delete potentially incriminating information, but could later challenge the federal government's ability to use decrypted information. This method will allow the alleged offender the opportunity to protect his own interest while recognizing the need for law enforcement officers to obtain evidence.

4. *CESA's Proposal for Law Enforcement Tools is Detrimental to the Value of Privacy*

CESA provides $80 million in appropriations for the Technical Support Center in the Federal Bureau of Investigation to respond to the increasing use of encryption by criminals.[155] The government justifies this need to develop abilities to decrypt encrypted data by stating that law enforcement agents have tools for collecting evidence of illegal activity, but these tools do not work if a party has not stored a decryption key with a recovery agent.[156] Because encryption codes the plaintext of data, if a key is not stored, this plaintext is unattainable. The government argues that access to plaintext is necessary to provide appropriate and necessary protection in cyberspace.[157]

Allocating $80 million to fund the ability to decrypt data strikes at the heart of America's value of privacy.[158] If a party intended encrypted

154. Faretta v. California, 422 U.S. 806, (1975) (explaining that notice to the accused is one of the foundations of due process, and this notice constitutionalizes the right to a fair adversarial trial).

155. *See* CESA, *supra* note 29, § 207 (setting forth an allocation of financial resources to develop methods for decrypting encrypted information). This provision of CESA does not specify the duties or goals of this program, however, § 207 allocates funds as follows: "(1) $25,000,000 for fiscal year 2000 for building and personnel costs; (2) $20,000,000 for fiscal year 2001 for personnel and equipment costs; (3) $20,000,000 for fiscal year 2002; and (4) $20,000,000 for fiscal year 2003." *Id.*

156. *See The Clinton Administration's White Paper*, *supra* note 27.

157. *See id.* (allowing for the Technical Support Center to develop means to decrypt encrypted data without obtaining a key).

158. *See* CESA, *supra* note 29, § 207 (allocating resources to develop decryption methods).

data to be decrypted by parties without a key, that party would not have encrypted the data in the first place. Essentially, CESA creates the same effect as the Clipper Chip by providing the government with the right and tools to decrypt data when a citizen chooses not to store a key with a recovery agent.[159] The Clipper Chip legislation, requiring key escrow, was vehemently opposed.[160] It is essential to keep in mind that the first transgression on individual liberties, no matter how small, opens the door for other transgressions.[161] CESA is seizing more than information. CESA is eliminating an individual's choice to protect his or her individual thoughts and ideas from government intrusion.

It is possible for CESA to preserve free choice while allowing the government to decrypt data without a key stored with a recovery agent. Law enforcement officials could provide notice of the search and request the alleged offender's permission to decrypt the data. Upon the alleged offender's refusal, law enforcement officials should be required to present a warrant to decrypt the data. This method provides the alleged offender with a choice to refuse decryption. Then, only upon a probable cause—based warrant could the information in question be decrypted. Even if law enforcement officers argue that exigent circumstances are present justifying the need for a warrantless search, at minimum, probable cause should be mandatory. However, the government should be required to obtain a warrant at the outset, to unquestionably support the legality of the search and seizure. This process would simply act as a safeguard ensuring freedom of choice for the alleged offender.

B. CESA Resolves Legal Issues Dealing with Third-Party Storage of Keys

CESA provides some protection for decryption keys stored with third party recovery agents[162] by establishing limitations on the government

159. *See* Brown & Tillett, *supra* note 115, at 1 (explaining that through the allocation of funds to develop decryption techniques, CESA provides that if keys are not stored with a recovery agent, the government has the right, upon proper procedures, to decrypt data as soon as the technology allows).

160. *See id.* (noting that the Clipper Chip which was designed to "protect private communications" while providing a "'backdoor' for law enforcement officials to decrypt necessary data."). The Clipper Chip initiative ceased after outcry by privacy groups. *Id.* Further, the computer industry cautioned potential abuse of power by law enforcement agencies. *Id.* at 2.

161. U.S. v. Hamilton, 97 F. Supp. 123, 128-29 (S.D. W.Va 1951) (Moore, J., dissenting) (noting that "[t]he Bill of Rights secures liberties which are sacred and inviolable."). A transgression of the Bill of Rights that remains uncorrected could lead to the erosion of the privileges and immunities secured by the Bill of Rights. *Id.* If the Fourth Amendment is transgressed, other individual rights will also suffer.

162. *See* National Security Advisor Jim Steinberg, Attorney General Janet Reno, Deputy Secretary of Defense John Hamre, Under Secretary of Commerce Bill Reinsch, and

use and disclosure of these keys.[163] CESA also protects the confidentiality of government techniques used to obtain admissible evidence[164] and ensures that exclusive corporate information, such as trade secrets, can be protected at trial.[165] Keeping these methods confidential is justified since disclosure of law enforcement decryption techniques can compromise the law enforcement methods used to protect our national security and imperil future investigations.[166] CESA also protects individuals and businesses that store key information with third party recovery agents.[167] Despite CESA's benefits, many concerns exist.

C. CESA Raises Legal Concerns Relating to Its Effectiveness

1. *CESA Alters the Requirements for Notice*

CESA abolishes the Fourth Amendment notice requirement designated in the Bill of Rights.[168] Jurisprudence mandates a judge-issued warrant based on probable cause that a crime was committed and contemporaneous notice of the search.[169] Notice requires that the law enforcement

---

Chief Counselor For Privacy at OMB Peter Swire, *Press Briefing at the Briefing Room*, Sept. 16, 1999 [hereinafter *Press Briefing*] (visited Oct. 7, 1999) <http://www.epic.org/crypto/legislation/cesa/briefing.html>. It is questionable whom the stored decryption keys will be protected from. *Id.* It is highly unlikely that the government protecting disclosure of decryption keys from itself. *Id.* It is implausible that the government would impose criminal sanctions upon itself for receiving disclosure of recovery information from third parties. *Id.* Presumably, CESA is addressing disclosure to businesses, however, the language of CESA is ambiguous in this respect.

163. *See id.*; *see also* Appendix II (detailing the pertinent portion of CESA amending 18 U.S.C. § 2711 addressing the disclosure or use of stored recovery information and providing criminal sanctions for those who do not abide).

164. *See* CESA, *supra* note 29, § 203 (proposing amendment to 18 U.S.C. § 2716 which provides for confidentiality of government techniques used to gain access to information upon a court order if the court finds that disclosure will likely expose a method of investigation that could imperil future investigations or risk the nation's security).

165. *See id.* A few exceptions exist to this general rule that prohibits the government from disclosing trade secrets to assist with the government's access to encrypted information. *Id.* These exceptions include the disclosure to another government body, the essential need to access the encrypted information, consent by the owner of the trade secret, and court order mandating disclosure. *Id.*

166. *See Press Briefing*, *supra* note 162 and accompanying text.

167. *See id.* (explaining that CESA adds new privacy protections for key storage in that standards for obtaining the decryption key are set forth). CESA provides for both civil and criminal sanctions for a third party recovery agent's improper release of decryption key information. *Id.*; *see also* White House Document: Analysis The Cyberspace Electronic Security Act of 1999 (Sept. 13, 1999) (visited Oct. 7, 1999) <http://www.epic.org/crypto/legislation/cesa/analysis.html> (explaining that if an individual encrypts data and loses the decryption key or survivors need key access for legitimate reasons, the key is attainable by securing a court order).

168. *See If the Government Wants Your Data It Should Come to You for It*, 5 CDT Policy Post 19 (2) (Aug. 20, 1999).

169. *See id. See also* U.S. Const. amend. IV.

official conducting a search present the individual with the warrant and provide an accounting of the seized items.[170] CESA eliminates this traditional practice.[171] Without contemporaneous notice upon issuance of a warrant, the individual cannot object to agents exceeding the warrant's scope.[172] Under the traditional issuance of a warrant, notice provides an individual with the privilege of requesting that the judge order the search stopped[173] and subsequently request that the property be returned.[174] CESA eliminates all of these rights.[175]

The Right to Financial Privacy Act of 1978 ("RFPA") governs the transfer of financial records and provides confidentiality to depositors.[176] Like CESA, RFPA aims to strike a balance between privacy rights and the needs of law enforcement. Under RFPA, banks cannot disclose payment information to the government without a court order, and to inspect an individual's financial records, nearly all federal investigators

170. *See If The Government Wants Your Data It Should Come To You For It, supra* note 168, at 5.

171. *See* CESA, *supra* note 29, § 203 (providing for notice "within 90 days of the date on which the government obtains the recovery information."). The opportunity for postponed notice for an indefinite period of time is available upon the government's showing of "good cause" to a "court of competent jurisdiction." *Id.*

172. *See If the Government Wants Your Data It Should Come to You for It, supra* note 168, at 5.

173. *See id.; see generally* Elkins v. U.S., 364 U.S. 206 (1960) (holding that evidence obtained through an unreasonable search and seizure is inadmissible upon defendant's timely objection). Notice provides a defendant with the opportunity to challenge the admissibility of the contents of seizure. *Id.* However, if notice is delayed, potentially indefinitely, the defendant cannot timely object even if the evidence was obtained through an unreasonable search and seizure. *Id. See also* Weeks v. U.S., 232 U.S. 383 (1914) (adopting the exclusionary rule in federal cases). CESA's delayed notice provision prevents a suspect's timely objection to the search and seizure, even if it is unreasonable. *Id.* If an unreasonable search and seizure has taken place in violation of the Fourth Amendment, the fruits of the search may be excluded at trial. *Id. See also* Mapp v. Ohio, 367 U.S. 643 (1961) (extending the exclusionary rule to bind state courts). *See also* Burdeau v. McDowell, 265 U.S. 465 (1921). Evidence that is seized by private parties is not subject to the exclusionary rule. *Id.* Therefore, evidence seized and decrypted by third-party recovery agents is not subject to the exclusionary rule unless the recovery agent is acting as a government agent. The Fourth Amendment applies to a search and seizure by a private party acting in collusion with the government in order to allow the government to circumvent the requirements of a search warrant. CESA leaves unclear whether third-party recovery agents are considered agents of the government, or simply private parties. Therefore, whether the fruits of the search are admissible is unclear, at best. Clarity is essential for citizens to know and understand the law, it is only then that citizens can obey the law.

174. *See If the Government Wants Your Data It Should Come to You for It, supra* note 168, at 5.

175. *See id.* (explaining that decryption keys are sought without the cooperation or knowledge of the individual using encryption because CESA provides for delayed notice). *See also Initial CDT Analysis, supra* note 122 and accompanying text.

176. 12 U.S.C. §§ 3401 *et seq.* (1999), *amended by* P.L. 106-102, Nov. 12, 1999, 113 Stat 1338.

must provide formal written requests and contemporaneous notice to the individual.[177] This contemporaneous notice provides an individual with the opportunity to challenge the government's attempt to access financial records.[178] Like RFPA, CESA should provide contemporaneous notice to allow an alleged offender to object to the search or any actions by the agent beyond the scope of the warrant.[179] This would provide the alleged offender with the right to object to the search ensured by the traditional issuance of a warrant.[180]

2. *CESA's Language is Vague*

The terms "generally applicable law" and "constitutionally protected expectation of privacy" appear in CESA, but remain undefined despite the opportunity to provide definitions in section 204.[181] "Generally applicable law" is a standard by which the court determines if a person or governmental entity is authorized to use or obtain stored recovery information from a recovery agent.[182] The government's definition in analyzing this issue is vague, but clearly does not permit a state to lower the bar of access to this information below the CESA standard.[183]

The term "constitutionally protected expectation of privacy" also ap-

---

177. *See id.*

178. *See id.*

179. *See If the Government Wants Your Data It Should Come to You for It, supra* note 168, at 5.

180. *See id. See also* Franks v. Delaware, 438 U.S. 154, 155-56 (1978) (explaining that a defendant in a criminal proceeding does have a Fourth Amendment right to challenge a search warrant and request a hearing). To receive this hearing, the defendant must substantially show that a "false statement [was made in the warrant affidavit] knowingly and intentionally, or with reckless disregard for the truth, [and the] false statement [was] necessary to the finding of probable cause." *Id.* If the defendant can make such a showing, the request for hearing must be granted. *Id.* At the hearing on the warrant affidavit, if the defendant can show perjury or reckless disregard by a preponderance of the evidence, the false material must be set aside. *Id.* If the warrant affidavit's "remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit." *Id.*

181. CESA, *supra* note 29.

182. *Id.* at § 2711 (b)(1)(A)(ii).

183. *See id.* at § 2712; *see also Press Briefing, supra* note 167 (explaining that generally applicable law includes "any law that generally covers ownership, control, or use of property or information, such as contract, agency, property, and estate laws, but does not include laws specifically addressing ownership, control, or use of recovery information only, or laws that support access to information in criminal investigations only"). While the "generally applicable law" standard is limited in explanation, this standard encompasses a wide variety of law. *Id.* Its scope is unclear because the boundaries are unknown. *Id.* It is unclear that § 2712 "would not allow a State to pass a law lowering standards of access below those set by new section 2717." *Id.*

pears undefined.[184] While CESA clearly states that no "constitutionally protected expectation of privacy" exists in the plaintext of encrypted information, CESA does not explain the scope of this term or how information becomes constitutionally protected by an expectation of privacy.[185] "Constitutionally protected expectation of privacy" is used in the section dealing with government access to escrowed keys for decryption.[186] Is there also not a constitutionally protected expectation of privacy if keys are not escrowed but data is encrypted?[187] The specific circumstances surrounding when data is protected remain unclear at best.[188]

The vague language used in CESA is analogous to the vague language used in the provisions of the Communications Decency Act ("CDA") that were held unconstitutional by the U.S. Supreme Court.[189] Despite the fact that the government had a compelling interest[190] to protect minors from exposure to sexually explicit,[191] "indecent," or "patently offensive" material[192] on the Internet,[193] the CDA was simply not narrowly tailored to achieve its goal[194] without abridging constitutional freedoms guaranteed to adults.[195] Because CESA contains vague language, it will likely face a similar fate. While the CDA did not attempt to regulate encryption, both statutes impose regulations on cyberspace and contain vague language.

Congress was not consistent in defining the terms "indecent" and "patently offensive" within the CDA, resulting in confusion about the

184. CESA, *supra* note 29, § 204.

185. *Id.* at § 2712(b)(4).

186. *Id.*

187. *See id.*

188. *See Proposal Also Sets Standards for Access to Escrowed Keys*, 5 CDT POLICY POST 19 (3) (Aug. 20, 1999) (stating that CESA's procedures are "complicated and unique, turning on unanswered questions of what is 'generally applicable law' and what is a 'constitutionally protected expectation of privacy.'"). *See also* Rachel Chalmers, *White House Proposes New Computer Surveillance Plan*, NETWORK WEEK, Aug. 23, 1999.

189. *See* Reno v. ACLU, 521 U.S. 844, 865-66 (1997) (holding that portions of the CDA were unconstitutional).

190. *See id.* at 872 (noting the government's legitimate interest in protecting minors). *See also id.* at 866 (noting the District court's finding of a compelling interest).

191. *See* Shea v. Reno, 930 F. Supp. 916, 922 (S.D.N.Y. 1996), *aff'd without op.*, Reno v. Shea, 521 U.S. 1113 (1997) (defining sexually explicit as Internet content depicting "sexual or excretory activities or organs" not exclusively in a patently offensive manner).

192. *Id.* Congress' interest in drafting the CDA was to limit on-line exposure of children to sexually explicit, though not legally obscene, materials available. *Id.*

193. *Id.* at 925-26. *See also* American Libraries Association v. Pataki, 969 F. Supp. 160, 164 (S.D.N.Y. 1997).

194. *See Reno*, 521 U.S. at 872-80 (explaining that the government's valid interest did not outweigh the inherent flaws within the CDA because the CDA was not narrowly tailored enough to accomplish its interest and did not employ the least restrictive means of doing so).

195. *See id.* at 872-80. The CDA abridged First Amendment freedoms of adults. *Id.*

meaning of these terms and their interconnection.[196] Therefore, the Court held in *ACLU v. Reno* that portions of the CDA were unconstitutionally vague.[197] *Reno's* holding was not surprising since both *Miller v. California*[198] and *Pope v. Illinois*,[199] earlier cases addressing an issue similar to the CDA, explain that clear language is essential.[200] Definite boundaries enabling an individual to know when he has violated the statute are necessary for a statute to pass constitutional muster.[201] A statute vaguely defining, or failing to define terms, encourages arbitrary prosecutions and is accordingly invalid.[202]

For CESA to pass constitutional muster, it must abide by precedent requiring that definite boundaries be ascertained enabling an individual to know when he has violated the statute. This can only be accomplished through clear definitions. By defining generally applicable law to mean that the FBI is the only governmental entity authorized to use or obtain stored recovery information from a recovery agent, the possibility of other government agencies obtaining access to such information is eliminated.[203] Vagueness can also be eliminated by specifying that "constitutionally protected expectation of privacy" does not include statutorily protected privacy rights and by detailing how information can be protected by an individual exercising their constitutional right to privacy.[204]

---

196. *Id.* at 872.

197. *Id.* (determining that the CDA was unconstitutionally vague and overbroad because it was not narrowly tailored enough to accomplish a compelling governmental interest).

198. 413 U.S. 15, 28 n.10 (1973) (explaining that to pass Constitutional muster, the language must "convey [a] sufficiently definite warning as to the proscribed conduct when measured by common understanding and practices" ascertaining boundaries).

199. 481 U.S. 497, 515 (1987) To pass constitutional muster, a statutory definition must explain the offense with "sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *Id.*

200. *See id.*

201. *See id.*

202. *See id.*

203. *See* CESA, *supra* note 29, §2711(b)(1)(A)(ii).

204. U.S. v. Anderson, 154 F.3d 1225,1229 (10th Cir. 1998), *cert. denied*, 119 S. Ct. 2048 (explaining that legitimate constitutional expectation of privacy exists if the defendant can "show a subjective expectation of privacy in the area searched, and second, that expectation must be one that society is prepared to recognize as 'reasonable'" in light of the surrounding circumstances). *See also* Katz v. U.S., 389 U.S. 347, 361 (1967) (Harlan, J., concurring). *See also* U.S. v. Jimenez, 894 F.2d 1, 5 (1st Cir. 1990). *See also* U.S. v. Hambrick, 55 F. Supp.2d 504, 507 (W.D. Va. 1999) (explaining that a risk analysis approach to the Fourth Amendment is necessary in determining a reasonable expectation of privacy).

3. *CESA Will Negatively Impact Companies*

CESA allows law enforcement officers to enter offices of the suspected criminal to search computers or a network server for evidence of criminal activity.[205] The law enforcement officer may then install software to defeat encryption.[206] While the encryption software appears to work, the data is not actually being encrypted.[207] The law enforcement official may then remove what is needed without having to decrypt data.[208] The problem with this method exists because company security is compromised.[209] If the alleged offender is a bank or other financial institution, personal financial records are opened and customers do not receive the privacy they paid for in choosing that company.[210] Further, the process itself is dangerous in that the law enforcement official could unintentionally devastate the company's computer system in searching a network server.[211] Additionally, once information is decrypted, CESA provides for its destruction[212] along with the destruction of essential, but non-incriminating information.

The implementation of this mandatory destruction provision can be devastating for parties turning over encrypted information. All decrypted information is destroyed, whether it is incriminating or not. To prevent the adverse impact of this provision, CESA should also provide for mandatory back up of encrypted information before decryption and destruction.

4. *CESA Will Drive Individuals to Seek Protection from Other Countries*

CESA will not solve the problem of criminals masking their activity through encryption because privacy will be sought from other coun-

205. *See* Rash, *supra* note 31.

206. *See id.*

207. *See id.*

208. *See id* at 5.

209. *See id.*

210. *See id.*

211. *See* Rash, *supra* note 31. Although the "Justice Department will say that such things [such as a government operative scrambling your data or bringing down your computer system] will never happen, but do they understand your computer installation well enough to know?" *Id.*

212. *See* CESA, *supra* note 29, § 2713 (providing for the destruction of recovery information unless otherwise specified in a court order). This provision asserts that if recovery information is provided to the government by a recovery agent or other person or entity, this party "shall destroy such recovery information in its possession and the government entity shall make a record documenting the destruction . . . ." *Id.* If the recovery information is destroyed, other necessary data may be lost to the detriment of the company. *Id.* A court order does not provide for preserving this recovery information. *Id.*

tries.[213] A Canadian privacy firm using remote servers and a complex network of encoding is one alternative available to U.S. citizens to protect their information from the U.S government.[214] Rather than leading privacy technology, the U.S. is attempting to evade it through CESA, causing U.S. citizens to look to other countries for privacy protection.[215]

Similarly, when the FDA has failed to approve certain drugs or herbal supplements, American citizens have sought these drugs from other countries, regardless of the potential danger involved in taking a substance not approved by the FDA. Similarly, because CESA can only effect privacy technology within the borders of the United States, if enacted, CESA will only encourage criminals to seek privacy technology from other countries. This will render the prohibition ineffective unless the government criminalizes the use of encryption software. Making the use of privacy technology illegal would place the federal government firmly in the shoes of Big Brother.

5. *CESA Regulates Encryption but not Other Similar Methods*

Encryption is narrowly defined by CESA as electronically transforming data to hide or obscure its readability.[216] CESA's definition does not include clearly visible messages since they do not hide any text. A method of coding that does not hide the content of the message would not be regulated by CESA, thereby providing a loophole for criminals to maintain confidentiality without violating CESA.[217] This method is known as chaffing and winnowing.[218]

Chaffing and winnowing evades CESA's regulations by using elec-

---

213. *See* Martin Stone, *Govt. Home Invasion Bill Drives US PC Users To Canada, Newsbytes News Network*, Aug. 24, 1999, *available at* 1999 WL 20019126. CESA has driven "tens of thousands of Americans to request privacy protection from Canadian firm Zero Knowledge Systems." *Id.* Zero Knowledge Systems provides what is known as the "only fully trustworthy privacy solution." *Id.*

214. *See id.* (noting the irony in American citizens seeking privacy from a Canadian company to protect them from strong centralized government control).

215. *See id.* (quoting David Sobel, general counsel for the Electronic Privacy Information Center). "It's disappointing that U.S. consumers must look to other countries for protection from a government they feel is overstepping its investigative authority." *Id. See also Home Invasion Bill Drives U.S. Computer Users To Canadian Privacy Firm Zero Knowledge Systems. Zero Knowledge Bombarded With Requests to Release Freedom Following Disclosure of 'Cyberspace Electronic Security Act,'* EDGE: WORK-GROUP COMPUTING REPORT, Aug. 30, 1999, *available in* 1999 WL 8113908.

216. CESA, *supra* note 29, § 204 (defining encryption as an "electronic transformation of data" to obscure or hide its plaintext).

217. *See id.*

218. *See* Ronald L. Rivest, *Chaffing and Winnowing: Confidentiality Without Encryption*, (visited Oct. 10, 1999) <http://theory.lcs.mit.edu/rivest/chaffing.txt>.

tronic authentication codes instead of encryption[219] to guard confidential data or communications.[220] Chaffing and winnowing operates by electronically sending a message in a combination of wheat (good packets) and chaff (bad packets).[221] First, chaff must be added to the original message to authenticate it.[222] Second, the receiver must remove the chaff to expose the original message.[223] A third party not aware of the authentication key cannot determine what is wheat and what is chaff,[224] therefore, the original text is indecipherable.[225] Chaffing and winnowing is analogous to an individual legally purchasing a pair of gloves,[226] and having a burglar use them to eliminate the possibility of leaving fingerprints at a crime-scene.[227] Through chaffing and winnowing, criminals can legally circumvent CESA, thus limiting its ability to prevent crime.[228]

---

219. *See id.* at 1, 6. No encryption occurs because the software simply authenticates messages by adding message authentication codes ("MACs") instead of using ciphers. *Id.*

220. *See id.* at 1-2.

221. *See id.* at 2. The chaff packets are additional packets with false MACs that are added into the correct overall format and logical message contents, but the chaff packets have invalid MACs. *Id.* Chaff packets are combined with the wheat packets. *Id.* Together they create a complete sequence. *Id.* The chaff may then be removed to reveal only the wheat. *Id.* The wheat revealed displays the original message. *Id.*

222. *See id.* at 1-2.

223. *See id.* A key is shared by the sender and receiver to "authenticate the origin and contents of each packet—the legitimate receiver, knowing the secret authentication key, can determine that a packet is authentic by re-computing the MAC and comparing it to the received MAC." *Id.* The packet and its MAC are instantly discarded if the comparison fails. *Id.*

224. *See* Rivest, *supra* note 218, at 3.

225. *See id.*

226. *See* Kurt M. Saunders, *The Regulation of Internet Encryption Technologies: Separating the Wheat From The Chaff*, 17 J. MARSHALL J. COMPUTER & INFO. L. 945, 957 (1999) (explaining that where gloves are hand-protection technology, winnowing and chaffing is data-protection technology that, to be regulated, would require the access of all authentication keys, similar to requiring sewn latex copies of an individual's fingerprints into the gloves).

227. *See id.*

228. *See* Mildred Guss, *New Crime-Fighting Law Should Trouble Everyone,* ALLENTOWN MORNING CALL, Aug. 26, 1999, at A18 (explaining that CESA will not reduce crime). CESA will simply encourage criminals to revert to the methods used in the pre-computer age or find loopholes through CESA to evade the law. *Id.*; *cf.* Louis J. Freeh, Director Federal Bureau of Investigation, Statement Before the Permanent Select Committee on Intelligence United States House of Representatives (Sept. 9, 1997), *available at* (visited Oct. 28, 1999) <http://www.fbi.gov/pressrm/ congress/97archives/encrypt14.htm> (noting that even legislation like CESA will not prevent criminals from achieving their acts). "No one contends that the adoption of a balanced encryption policy will prevent all criminals, spies and terrorists from gaining access to and using unbreakable encryption." *Id.* "But if we, as a nation, act responsibly and only build systems and encryption products that support and include appropriate decryption features, all facets of the public's interest can be served." *Id.*

6. *CESA Strikes at the Heart of Privacy Values and the Fourth Amendment*

Just as the American colonists were victims of the unrestricted search of their homes by British soldiers,[229] if CESA is passed, law-abiding American citizens will be the casualties of these modern searches.[230] Under CESA, federal agents will be able to search anyone's computer,[231] which many consider an extension of their home. Computers house personal diaries, personal communication, and treasured documents, similar to the colonists' homes and offices. As is evident from past warrant problems,[232] narrowly targeted search warrant requirements must be obeyed to protect individual rights and to minimize the issuance of warrants being issued against innocent citizens.[233]

CESA's effect on private citizens will be similar to the seizure laws that attacked drug trafficking in the 1980s.[234] These drug trafficking laws allowed law enforcement officials to seize personal belongings of individuals related to suspected drug crimes without the mandate of a trial or a formal filing of charges.[235] These seizure laws, intending to target and punish drug dealers, frequently penalized private law-abiding citizens on the basis of mere suspicion.[236] Similarly, in the age of cyberspace, law-abiding citizens attempting to protect their privacy through encryption may face a law enforcement "open season" if CESA is passed.[237] Mere suspicion will be enough for comprehensive computer surveillance or searches.[238] The victims, as with the drug trafficking legislation of the 1980s, will frequently be law-abiding citizens.

In the debate between privacy and surveillance, surveillance supporters argue that criminals and persons attempting to hide unfavorable conduct are the only ones who should be concerned about privacy.[239] However, even law-abiding citizens can suffer harms from disclosure of personal information.[240] The disclosure of financial transactions to the

---

229. *See supra* notes 70-74 and accompanying text.

230. *See* Glasser, *supra* note 69, at 638.

231. *See Justice Dept. Seeks New Encryption-Related Authority, Communications Daily*, Aug. 20, 1999, *available at* 1999 WL 7580219.

232. *See* Glasser & Schwartz, *supra* note 102 and accompanying text.

233. *See id.*

234. *See* Joe Wilcox, *Justice Wants Broader Computer Search Liberties*, CNET NEWS.COM (Aug. 20, 1999) <http://news.cnet.com/category/0-1005-200-346284.html>.

235. *See id.*

236. *See id.*

237. *Id.*

238. *See id.*

239. *See* Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 473 (1999).

240. *See id.* at 473 Many of the current methods of surveillance technology that intrude on privacy are perfectly legal. *Id.*

government can result in the use of this information for economic or political advantage against the politically powerless who may then become targets for government exploitation.[241] Citizens who fear the negative use of their personal information may forego transacting in cyberspace altogether because they do not feel free to go against the government's wishes, even though their activities may be perfectly legal.[242] This effect may be similar to that of a totalitarian regime where the fear of detection and punishment, even when unwarranted, results in a chilling effect on personal expression.[243] In turn, the American economy may suffer negative impacts because of the fear of unsecured transactions in cyberspace.[244]

D. THE GOVERNMENT IS TAKING ON A BIG BROTHER ROLE THROUGH CESA

You have zero privacy anyway. Get over it.[245]

1. *CESA Will Alter Traditional Warrant Requirements*

CESA specifically states that there is no constitutionally protected expectation of privacy in the plaintext of data.[246] From case law, a test emerged determining when a warrant for a search is necessary and when it is not.[247] Whether there is a legitimate expectation of privacy in

241. *See id.* at 473.

242. *See id.* at 474.

243. *See id.* at 474. Even desirable behavior may be chilled out of fear. *Id.* Consumers who fear the surveillance of their financial transactions may forego Internet purchases or on-line banking. *Id.* Individuals may begin transacting with cash more frequently because it is less traceable and provides more anonymity. *Id.* Further, this fear of "being watched" may cause heavy psychological burdens on American citizens. *Id. See also* Jed Rubenfeld, *Contemporary Challenges To Privacy Rights*, 43 N.Y.L. SCH. L. REV. 195, 214-15 (1999) (explaining that totalitarianism is an anti-democratic means by which the government dictates individual lives). If the majority passes a totalitarian-like law, then the law is also anti-democratic and a means of governmental control over individual lives. *Id.* "[P]rivacy . . . is an anti-totalitarian principle" that is necessary to the American democracy. *Id.* If the American government passes a law hindering one's right to privacy, it is acting in a totalitarian manner. *Id.* CESA potentially hinders the privacy rights of law-abiding American citizens.

244. *See id. See also* Jonathan P. Cody, *Protecting Privacy Over The Internet: Has The Time Come To Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1183-84 (1999) (noting that the primary reason for foregoing Internet communications and transactions is individual concerns about privacy).

245. Erika S. Koster, *Zero Privacy: Personal Data On The Internet*, 16 No. 5 COMPUTER L. 7 (May, 1999) (quoting Sun Microsystems CEO Scott McNealy, talking to a group of reporters about his 'Jini' Java project, reported in WIRED NEWS (Mar. 11, 1999)).

246. *See* CESA, *supra* note 29, § 204 (failing to define the term "Constitutionally protected expectation of privacy.").

247. *See* U.S. v. Anderson, 154 F.3d 1225, 1229 (10th Cir. 1998) (explaining that a warrantless search is unreasonable if the "defendant has a legitimate expectation of privacy in

stored data remains unclear. If there is no legitimate expectation of privacy in the data, no warrant is necessary. However, the language of CESA should indicate whether encrypted information has a reasonable expectation of privacy associated with it. If a warrant is necessary because a reasonable expectation of privacy exists, the risk-analysis approach to the Fourth Amendment applies.[248] The validity of a search may only be challenged by asserting a subjective expectation of privacy that is based on an objective standard of reasonableness. If no subjective expectation of privacy exists, the search and seizure may not be challenged.[249] Because there is no expectation of privacy in the plaintext of

---

the area searched."). This legitimate expectation of privacy exists if the defendant can "show a subjective expectation of privacy in the area searched, and second, that expectation must be one that society is [objectively] prepared to recognize as 'reasonable'" in light of the surrounding circumstances. *Id.* *See also* Smith v. Maryland, 442 U.S. 735, 744-45 (1979); *see also* U.S. v. Fultz, 146 F.3d 1102, 1106 (9th Cir. 1998) (holding that a homeless individual has a reasonable expectation of privacy in a closed cardboard box stored inside another individual's garage). The court reasoned that a homeless individual, who cannot afford a suitcase, purse, or other container, likely stores his/her own private belongings in a box similar to how an established individual stores his/her own private belongings in his/her purse or container within his/her home. *Id.* Therefore, it can be analogized that a personal computer within an individual's home also carries with it a reasonable expectation of privacy. *Id.* The CESA standard would reject the above reasoning. CESA's standard maintains that there is no constitutionally protected expectation of privacy in the plaintext of data. *Id.* Then does CESA also mean that there is no legitimate expectation of privacy under case law, thereby eliminating the need for a warrant? If so, CESA has created an unnecessary warrant requirement.

248. *See* U.S. v. Hambrick, 55 F. Supp.2d 504, 507 (W.D. Va. 1999) (holding that an Internet Service Provider ("ISP") could reveal biographical and financial information to the government without violating the Fourth Amendment). *Hambrick* explained that a registered name on an account and the credit card securing the account could be disclosed since *Hambrick* voluntarily furnished that information to the ISP, thereby assuming the risk that his personal information may be disclosed to law enforcement officers. *Id.* "For Internet customer[s] to have a reasonable expectation of privacy in . . . [their] personal information under risk-analysis approach to Fourth Amendment: (1) data must not be knowingly exposed to others, and (2) Internet service provider's ability to access data must not constitute disclosure." *Id.* at 504-508. CESA finds that escrowing a key with a third party is disclosure. While *Hambrick* states that the "Internet service provider's ability to access data must not constitute disclosure" it remains unclear whether CESA's intention is that escrowing a key is disclosure because the Internet provider has the ability to access the data. *Id.* If so, then the *Hambrick* test and CESA are inconsistent. *Id.* Therefore, under CESA, no reasonable expectation of privacy in an individual's personal information can ever be attained under the risk-analysis approach to the Fourth Amendment. *Id.* Further, because encryption is defined as information that is hidden and not knowingly exposed to others, is the definition of encryption altered by an individual's choice to store a decryption key with a third party? These issues are unresolved by CESA.

249. *See* Smith v. Maryland, 442 U.S. 735, 740-741 (June 1979) (explaining that the Court has consistently held that whether the Fourth Amendment applies depends on whether the individual invoking its protection "can [objectively] claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."). *See also* Rakas v. Illinois, 439 U.S. 128, 150-51 (1978), (concurring opinion); *see*

data,[250] the alleged offender may not challenge the warrant and subsequent search and seizure, thereby allowing the government to control the lives of its citizens without challenge.[251]

If issuing a warrant is necessary, it must be done with specific particularity so that an executing officer reading the warrant would reasonably know what items to seize.[252] Problems arise under CESA because the files containing data are encrypted. It is unlikely that an individual choosing to use encryption would not encode the file name. Thus, a warrant particularly describing that all coded files could be seized would provide access to personal non-incriminating encrypted information, thus placing an individual's reasonable subjective expectation of privacy under an objective standard. An individual would be unable to challenge the seizure even if a warrant is necessary under CESA's delayed notice provision.[253] If a warrant is not required under CESA's unique standard, because there is "no constitutional privacy interest in the plaintext," the seizure could not be challenged.[254] Regardless of whether a warrant is required, the seizure may not be challenged,[255] implying that government interests are paramount to the rights of individuals. This issue strikes at the very heart of the Fourth Amendment debate on this matter — will the limited privacy right essential to democracy be preserved or will it be circumvented by CESA?[256]

---

also id. at 164 (dissenting opinion); *see also* U.S. v. Chadwick, 433 U.S. 1, 7 (1977); *see also* U.S. v. Miller, 425 U.S. 435, 442 (1976); *see also* U.S. v. Dionisio, 410 U.S. 1, 14 (1973); *see also* Couch v. U.S., 409 U.S. 322, 335-336 (1973); *see also* U.S. v. White, 401 U.S. 745, 752 (1971) (plurality opinion). Two questions must be satisfied under the "reasonable expectation of privacy" test to invoke Fourth Amendment protection. *Id.* First, it must be determined whether the individual's conduct exhibits "an actual (subjective) expectation of privacy" by showing that he/she seeks to preserve something as private. *Id.* Second, the court must determine whether the subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable'" if objectively examined. *Id. See, e.g.*, Rakas v. Illinois, 439 U.S. at 143 n.12.

250. *See Initial CDT Analysis*, *supra* note 122, at 2.

251. *See* U.S. v. Maxwell Jr., 45 M.J. 406, 417 (1996).

252. *See* U.S. v. Hall, 142 F.3d 988, 996 (7th Cir. 1998).

253. *See* CESA, *supra* note 29, § 203 (describing proposed 18 U.S.C. § 2714).

254. Jennings, *supra* note 119 and accompanying text.

255. *See id.*

256. *See* Joel R. Reidenberg, *Restoring Americans' Privacy In Electronic Commerce*, 14 BERKLEY TECH. L.J. 771, 775 (1999); *cf.* Robert MacMillan, *Crypto Preoccupies Army, Weldon - Update*, Sept. 29, 1999, at 2 (noting that CESA is a hidden agenda by which the federal government is providing a bill to satisfy the law enforcement supporters who are uneasy over criminal use of encryption).

2. *CESA Will Decrease Privacy, Thereby Impairing the Growth of Cyberspace*

CESA's attempt to play Big Brother will impact the American population by causing greater concern that information and communications will not be private. Americans report that one of the main reasons they avoid using the World Wide Web is the fear that others may access their personal information.[257] It is necessary to note that this statistic was recorded before encryption regulations under CESA were proposed.[258] If CESA is passed, even less privacy will exist.[259] Concern regarding the lack of privacy in communications transmitted over networks, through cyberspace, and through storage in computers will increase. These concerns are warranted.[260]

Currently, American citizens may protect the privacy of their computer files, Internet transactions, and communications by using encryption.[261] CESA will take away some of this freedom by providing

257. *See* Reidenberg, *supra* note 256, at 771-72 (explaining that "the fair treatment of personal information and citizen confidence in such treatment are each necessary conditions for electronic commerce over the next decade" that if ignored, will detrimentally effect electronic commerce as we know it). CESA is a prime example of the "narrow, ad hoc legal rights enacted in response to particular scandals involving abusive information practices." *Id.* "The approach has led to incoherence and significant gaps in the protection of citizens' privacy." *Id.* "For example, substance abusers have stronger privacy rights than web users in the United States." *Id.* Rather than revise current privacy legislation, the federal government is responding ad hoc to the issues raised by the encryption debate. *Id.* This response will inhibit the growth of Cyberspace. *Id.* at 772. *See also* Andrew L. Shapiro, *Privacy for Sale: Peddling Data on the Internet*, 26-WTR HUM. RTS. 10. "[A] 1995 Louis Harris poll found that 82 percent of respondents were concerned about their personal privacy." *Id.* The concern over privacy reflects the emergence of private surveillance. *Id.* With government surveillance compounding the equation, concern for personal privacy may only increase. *Id.*

258. *See* Reidenberg, *supra* note 256, at 772.

259. *See* Swire, *supra* note 239, at 463 (explaining that government access to information individuals intend to keep private may result in discriminatory effects). "New accumulations of data may be disproportionately used against the weak by the strong." *Id.*

260. *See* Chris Cobbs, *Does Uncle Sam Want To Be Your Big Brother*, ORLANDO SENTINEL, Nov. 21, 1999 at G1 (explaining that CESA raises a contemporary version of the age old dilemma, "how far can government go in providing security for all when it clashes with personal privacy . . . and who makes sure it doesn't go too far?"). The government argues the need for CESA because Cyberspace inherently provides centralized and accessible information virtually anonymously, and encryption inherently conceals this information or communication. *Id.* The government recognizes that as Cyberspace develops creating a new medium without traditional boundaries, the government has an opportunity to expand its search and seizure powers. *Id.* "Not only is Big Brother watching, but he's watching in ways unimaginable a few years ago." *Id.* It is necessary to establish privacy legislation that entitles individuals to defend their privacy. *Id.*

261. *See* Americans For Computer Privacy, *Encryption and Your Right to Privacy* (visited Feb. 28, 2000) <http://www.computerprivacy.org/choice.cgi>.

government with a means to access both data and communications.[262] CESA allows a government official to demand encryption keys from third parties.[263] If a key held by a third party is not available, the government will have a means of decrypting information through decryption technology developed by the FBI and the Justice Department.[264] The ability for government to access encrypted data and communications, regardless of whether a key is stored with a third party, is a threat to individual privacy. This threat to privacy is analogous to the government telling an individual to leave his front door key with a neighbor, who may then be required to give that key to the government.[265] If a front door key were not given to a neighbor, law enforcement officials would then have the right to pick the lock and search the individual's home. The impact is that individuals may well choose to abstain from communicating and transacting in cyberspace in order to protect privacy.[266] Logic dictates that communications, commerce, and the economy as a whole, will suffer if individuals abstain from communicating and transacting in cyberspace. Consequently, the nature of society may change for the worse if surveillance, rather than privacy, is encouraged.[267]

D. Proposed Redrafting of CESA

Through this analysis, it is evident that CESA is the government's attempt at taking on a Big Brother role. However, CESA can be redrafted and narrowly tailored to accomplish its goal of enabling law enforcement to obtain access to encrypted information while protecting individual privacy rights. It is necessary, in redrafting CESA, to maintain awareness that technology is continuously changing, as is the manner in which citizens use technology.[268] These changes warrant careful attention to drafting laws that can evolve with changing technologies without eroding the basic protections provided by the Fourth Amendment. This can be accomplished by altering CESA's unique notice standard. CESA's notice standard should be consistent with the traditional notice standards that have endured. Individuals reasonably expect that when they encrypt data, the privacy of their data is secure. CESA can guarantee an individual's expectation of privacy while allowing law enforcement officers to achieve their objectives by providing contemporaneous notice to an individual that his computer will be searched and any

262. *See id.*
263. *See id.*
264. *See id.*
265. *See id.*
266. *See* Hunter, *supra* note 51, at 198 (explaining that the lack of secure encryption technology will cause individuals and organizations alike to forego online communication).
267. *See* Swire, *supra* note 239, at 463.
268. *See* Berman & Mulligan, *supra* note 37, at 569.

encrypted data or communications will be decrypted. Once law enforcement officials decrypt the crucial portion of the encrypted data, the individual's information should not be improperly altered or destroyed without the individual's permission. By providing these safeguards to individual privacy, individuals will have a form of redress if they are harmed by improper government intrusion.[269] This method would serve the governmental interest while providing individuals with a means to "check" unreasonable intrusion by the government.

Further, by defining the scope of "generally applicable law," the term "constitutionally protected expectation of privacy," and specifying whether plaintext of encrypted data is covered under a statutorily protected expectation of privacy or subject to traditional Fourth Amendment interpretation, CESA will more clearly delineate the new means of governing encryption technology in cyberspace. Further, including the winnowing and chaffing method in the definition of encryption will eliminate the loophole through which criminals may slip. CESA may then prevent individuals from using encryption to facilitate crime.

Even if these changes are made, CESA will still support the government taking on a Big Brother role through its watchful eye over personal information and communications. The American public can preclude the government from assuming this role by expecting and demanding privacy in cyberspace communications, transactions, and information.[270] If privacy in cyberspace becomes a reasonable expectation of American citizens, it will be protected, and the government's scope of authority will be

269. *Crafting a Balanced Legislative Proposal*, 6 CDT POLICY POST, No. 4 (last modified Feb. 16, 2000) <http://www.cdt.org/publications/pp_6.04.shtml>. From a privacy perspective, current technology laws do not provide American citizens with adequate redress against unwarranted government intrusions. *Id.* Under the 1986 Electronic Communications Privacy Act ("ECPA"), the rule against government monitoring of conversations between law-abiding citizens was weakened. *Id.* Stored data on networks are not given complete privacy protection under the ECPA. *Id.* Further, protections against using "illegally obtained evidence and the remedies for privacy violations, do not apply to email and other Internet communications." *Id.* The ECPA does not require notice to a customer if the government, by subpoena, requests personal information from an Internet Service Provider for a civil lawsuit. *Id.* Therefore, the customer is not provided with an opportunity to object until the information is in the hands of the government. *Id.* This method deprives an individual of the right to be heard. Under the current CESA proposal, the issue is not addressed. Privacy violations must be minimized. To minimize privacy violations, protection for email, data stored on networks, and Internet communications must be included in CESA. Only then are individual rights in Cyberspace secure. Each individual should be provided with the opportunity to be heard and object to the government's access to personal information. This opportunity can only be provided through adequate notice by the government to the individual prior to the issuance of a warrant.

270. *See* Hunter, *supra* note 51, at 207 (explaining that informing the public of eroding privacy protections in personal data, information, and communications will play a key role in how privacy is viewed in current legislative developments and judicial interpretation).

limited. Law-abiding American citizens do not have to become the victims of legislation responding to technology if that legislation compromises their right to privacy.[271] The American public must decide whether the government's actions are what our Founders envisioned when drafting the Fourth Amendment in response to colonial search and seizure practices.

IV. CONCLUSION

No lawful protection of privacy currently exists against government interception of electronic communications. Encryption is essential to maintaining the privacy of information during cyberspace communications.[272] Therefore, encryption is needed to preserve the Fourth Amendment right to protection from unreasonable search and seizure.[273] While encryption regulation is necessary, it is equally important to use caution in drafting legislation aimed at regulating encryption. CESA's current method allowing governmental access to decryption keys held by third parties and keyless means of decrypting data, based on CESA's unique statutory standard, would likely hinder America's economic growth by preventing E-commerce from reaching its potential.[274] Seeking to avoid unwarranted government intrusion and the disclosure of private information, businesses and law-abiding citizens may seek privacy protections outside of the United States.[275] This action would negatively affect the U.S. economy,[276] and national security would be compromised as criminals seek methods, not regulated by CESA, namely winnowing and chaffing, to protect their activities.[277] As proposed, CESA can provide limited safeguards to protect individuals' right to privacy while promoting the objectives of law enforcement officers by redrafting and narrowly tailoring the current draft of CESA.

The primary question is whether we as law-abiding U.S. citizens are willing to further limit our Fourth Amendment rights to security and privacy in order to provide the government with increased opportunities

271. *See id.* (quoting Cruzan v. Missouri Dep't of Health, 497 U.S. 261 (1990) (Brennan, J., dissenting)). "[L]aw, equity and justice must not . . . quail . . . in the face of modern technological marvels presenting questions hitherto unthought of . . . . [T]he bodies and preferences and memories of [individuals] do not escheat to the State; nor does our Constitution permit . . . any government to commandeer them." *Id.* at 210.

272. *See* Gwynne B. Barrett, *The Law of Diminishing Privacy Rights: Encryption Escrow and the Dilution of Associational Freedoms in Cyberspace*, 15 N.Y.L. SCH. J. HUM. RTS. 115, 139 (1998); *see also* 144 CONG. REC. S9419 (daily ed. July 30, 1998) (statement of Mr. Lott for Americans For Computer Privacy).

273. *See id.*

274. *See id.*

275. *See id.*

276. *See id.*

277. *See id.*

to uncover potential criminal activity in the Cyber Age.[278] The Fourth Amendment right to be free from unreasonable search and seizure is a well-established bedrock of American society that is so fundamental to individual liberty that it ought not be peddled away.[279]

Hillary Victor

278. *See* Richard S. Huleatt, *Clinton Administration Relaxes Encryption Restrictions*, INFORMATION INTELLIGENCE ONLINE NEWSLETTER, Oct. 1, 1999, at 1. CESA's failure to protect against illegal searches will leave the average law-abiding citizen out in the cold while advocating the government's ability to interfere with "any meaningful use of encryption that would [traditionally] be secure from government snooping or abuse." *Id.*

279. *See* Shapiro, *supra* note 257, at 11-12. As American citizens "[w]e do not buy and sell civil liberties." *Id.* In the words of Justice William O. Douglas, echoing Justice Louis Brandeis, "The right to be let alone is indeed the beginning of all freedom." *Id.* at 12. This view suggests that privacy rights carry a preferred status and should continue to do so in the future. *Id.*

APPENDIX I

Cyberspace Electronic Security Act of 1999 § 203 (Sept. 16, 1999) (last modified Sept. 17, 1999), *available at* <http://www.cdt.org/Crypto/CESA/CESArevised.shtml> (amending chapter 121 of Title 18 of the United States Code, in pertinent part). Section 203 of CESA is a proposed amendment to Chapter 121 of Title 18 to add §§ 2711 and 2712. Section 2712 provides in pertinent part:

Requirements for governmental access to, use of, and disclosure of stored recovery information;

(a) Compelled disclosure and use of stored recovery information in the possession of recovery agents. –A governmental entity may require a recovery agent to disclose stored recovery information to the governmental entity, or to use stored recovery information to decrypt data or communications—

(1) pursuant to a warrant issued pursuant to the Federal Rules of Criminal Procedure or an equivalent State warrant, or an order issued under section 2518 of this title;

(2) pursuant to any process under federal or State law to compel disclosure that is permitted by section 2711(b)(1)(A)(i); [which allows a recovery agent to disclose stored recovery information or to decrypt data communications with the consent of the person, entity, or agent of the entity storing the data];

(3) pursuant to a court order issued under subsection (b); or

(4) when an investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, reasonably determines that–

(A) an emergency situation exists that involves–

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime or terrorism, requiring that recovery information be obtained or used before an order authorizing the same can, with due diligence, be obtained; and

(B) there are grounds upon which an order could be entered under this section to authorize such disclosure by a recovery agent of stored recovery information, or the decryption of data or communications by a recovery agent using stored recovery information;

but an order under this section must be sought within forty-eight hours after the stored recovery information has been released or the decryption has occurred. In the event no order is requested within that time or the request for an order is denied, the governmental entity shall not further use or disclose the recovery information received or plaintext recovered, shall seal such information or plaintext under the direction of a court of competent jurisdiction, and shall serve notice as provided for in subsection (c) of this section;

A federal governmental entity may require a recovery agent to disclose stored recovery information to it or another federal governmental entity, or to use stored recovery information to decrypt data or communications, under paragraphs (1), (2), (3), or (4) for the benefit of a foreign government, pursuant to a request of a foreign government under applicable legislation, treaties, or other international agreements;

(b) Requirements for court order for disclosure or use of stored recovery information by a recovery agent. —A court order requiring a recovery agent to disclose stored recovery information to a governmental entity or to use stored recovery information to decrypt data or communications on behalf of a governmental entity shall be issued by a court of competent jurisdiction upon a finding, based on specific and articulable facts, that–

(1) the use of the stored recovery information is reasonably necessary to allow access to the plaintext of data or communications;

(2) such access is otherwise lawful;

(3) the governmental entity will seek such access within a reasonable time; and

(4) there is no constitutionally protected expectation of privacy in such plaintext, or the privacy interest created by such expectation has been overcome by consent, warrant, order, or other authority.

An order under this section directing the disclosure of stored recovery information shall be limited to the extent practicable to directing the disclosure of only that stored recovery information that is necessary to allow access to the plaintext of the relevant data and communications.

(c) Notice. –Within 90 days after receiving stored recovery information or decrypted data or communications from a recovery agent, the govern-

mental entity shall notify the person or entity, if known, who stored the recovery information that stored recovery information was disclosed or used by the recovery agent, and such notice shall state the date on which the stored recovery information or decrypted data and communications were disclosed. On the government's ex parte showing of good cause, the giving of notice may be postponed by a court of competent jurisdiction. Notice under this section shall be provided by personal service, or by delivery by registered or first-class mail . . . .

Id.

APPENDIX II

Cyberspace Electronic Security Act of 1999 § 203 (Sept. 16, 1999) (last modified Sept. 17, 1999), *available at* <http://www.cdt.org/Crypto/CESA/CESArevised.shtml>. Section 2711 provides in pertinent part:

(a) Prohibitions and requirements. —

(1) Except as provided in sections (b) and (d), a recovery agent shall not–

(A) disclose stored recovery information;

(B) use stored recovery information to decrypt data or communications; or

(C) disclose any other information or record that identifies a person or entity for whom the recovery agent holds or has held stored recovery information;

(2) No person or entity shall knowingly obtain stored recovery information from a recovery agent knowing or having reason to know he has no lawful authority to do so;

(3) A recovery agent shall inform any person or entity who stores recovery information with the recovery agent of the location or locations where the recovery information is stored.

(b) Authorizations for disclosure or use. –

(1) Recovery information. –A recovery agent may disclose stored recovery information, or use stored recovery information to decrypt data or communications, only–

(A) in the case of disclosure to or use on behalf of any person or entity, including a governmental entity–

(i) with the consent of the person or entity who stored such recovery information, or the agent of such person or entity; or

(ii) pursuant to an order of a court of competent jurisdiction, if such court has found that another person or entity is legally entitled pursuant to generally applicable law to receive, possess, or use such recovery information and has, if practicable, provided the person or entity who has stored the recovery information with an opportunity to be heard; or

(B) in the case of disclosure to or use on behalf of a governmental entity, as specified in section 2712 of this title.

(2) Customer information. –A recovery agent may disclose information or a record, other than stored recovery information, that identi-

fies a person or entity for whom the recovery agent holds or has held stored recovery information only–

(A) with the consent of the person or entity who stored such recovery information, or the agent of such person or entity;

(B) if the disclosure is necessarily incident to the rendition of the service provided to the person or entity who has stored such recovery information, or to the protection of the rights or property of the recovery agent;

(C) pursuant to an order of a court of competent jurisdiction based upon a showing of compelling need for the information, if such court has, if practicable, provided the person or entity who has stored such recovery information with an opportunity to be heard; or

(D) to a governmental entity pursuant to a warrant issued pursuant to the Federal Rules of Criminal Procedure or equivalent State warrant, a court order, or a federal or State subpoena; provided, however, that notice to the person or entity who stored such recovery information is not required under this subparagraph, and, furthermore, that a court of competent jurisdiction may for good cause order that the recovery agent not disclose the government request for 90 days, which period may be extended upon further showings of good cause.

(c) Confidentiality. –Except as otherwise provided by law, or by order of a court of competent jurisdiction, a recovery agent who is requested or ordered to disclose stored recovery information to, or to use stored recovery information on behalf of, a governmental entity pursuant to paragraph (b)(1) above shall not reveal to any person or entity the fact that the governmental entity has requested or received stored recovery information from, or has required the use of stored recovery information by, the recovery agent, and shall not disclose to any other person or entity any decrypted data or communications that are provided to the governmental entity.

(d) Exclusions. —Nothing in this section or section 2712 of this title shall be construed to prohibit a recovery agent from:

(1) except as provided in subsection (c), using or disclosing plaintext in its possession, custody, or control;

(2) using or disclosing recovery information that is not stored recovery information held by it under the circumstances described in section 2718(7); or

(3) using stored recovery information in its possession, custody or control to decrypt data or communications in its possession, custody,

> or control, if applicable statutes, regulations, or other legal authorities otherwise require the recovery agent to provide such data or communications to a governmental entity in plaintext or other form which can be readily understood by the governmental entity.

(e) Criminal sanctions. –Whoever knowingly violates or attempts to violate subsection (a) or subsection (c) of this section shall be fined under this title, or imprisoned for not more than one year, or both.

Id.