Taking Account of the World As it Will Be: The Shifting Course of U.S. Encryption Policy

Tricia E. Black*

* B.A., Indiana University—Bloomington, 1998, *summa cum laude*; candidate for J.D., Indiana University School of Law—Bloomington, 2001. Ms. Black wishes to thank her family and friends, especially Michael Hulka, for their support, and Roger Deetz for early explanations of technical issues in "teb terms." Ms. Black wishes to dedicate this Note to her grandmother, Helen Black, whose recent discovery of the Internet is an inspiration to never stop learning.

> It is change, continuing change, inevitable change, that is the dominant factor in society today. No sensible decision can be made any longer without taking into account not only the world as it is, but the world as it will be.[1]

I. INTRODUCTION

On January 12, 2000, the U.S. Department of Commerce Bureau of Export Regulation ("BXA") issued new encryption export regulations that removed most of the prior limitations on the export of U.S. encryption technology. The previous export limitations, combined with efforts by the Clinton Administration to encourage the use of key escrow, had sparked contentious debate among public interest privacy groups, law enforcement, and the high-tech software industry.[2] The relaxation in policy signaled another retreat by the Clinton Administration from strong restrictions on export technology. While some questioned the complicated nature of the regulations, one software executive characterized the liberalization as "an 'inside the ball park' home run."[3] The finalized regulations had been eagerly anticipated since September 16, 1999, when the White House announced its proposal to loosen restrictions ("September proposal"), perhaps because of increasing pressure from Congress through proposed legislation over the previous three years.[4]

In the wake of the new regulations and the furor that led to them, however, little mention has been made of the Cyberspace Electronic Security Act of 1999 ("CESA"), which was announced by the Clinton Administration in tandem with the September proposal to loosen export restrictions.[5] As proposed, CESA would "establish[] limitations on government use and disclosure of decryption keys obtained by court process and provide[] special protections for decryption keys stored with third party 'recovery agents,'" and authorize appropriations for a Federal Bureau of Investigations ("FBI") Technical Support Center to serve as a

1. Isaac Asimov, *My Own View*, *in* THE COLUMBIA DICTIONARY OF QUOTATIONS 129 (Robert Andrews ed., 1993).

2. *See* David E. Sanger & Jeri Clausing, *U.S. Removes More Limits on Encryption Technology*, N.Y. TIMES, Jan. 13, 2000, at C1.

3. *Id*. Dan Burton is "vice president of governmental relations at Novell, Inc., a leading software company which is based in Utah." *Id*.

4. John Schwartz, *U.S. Eases Encryption Export Rules*, WASH. POST, Jan. 13, 2000, at E1.

5. White House Press Release, *Administration Announces New Approach to Encryption* (Sept. 16, 1999), *at* http://www.epic.org/crypto/legislation/cesa/WH_release_9_16. html.

resource for federal, state, and local law enforcement.[6] Online privacy proponents strongly criticized CESA, claiming it would allow the government to circumvent the Fourth Amendment and easily gain access to encrypted e-mails, business documents and private files.[7] Former President Clinton left office without Congress taking any action on CESA, despite the White House's transmittal letter to Congress in September 1999.[8]

This Note argues that the marked changes in U.S. encryption policy in the past seven years, specifically the relaxation of export regulations and key escrow advocacy, result from governmental and societal recognition and acceptance of how the world will be in the information age. Despite these expansive actions, introduction of CESA signals yet another attempt at government regulation of encryption technology. Therefore, this Note encourages critical study of CESA and similar legislation to ensure public awareness, understanding, and active involvement in shaping encryption policies affecting those living and working in the interconnected twenty-first century. Part II of this Note offers a brief history of cryptography and explains modern terminology essential to comprehension of the encryption debate. Part III traces governmental regulation of encryption technology—until recently almost solely a creation of executive directive—and offers competing arguments regarding key escrow systems and restrictive export regulations. Part IV analyzes both facets of the September proposal: export relaxation and CESA. Finally, Part V argues that Internet advances have caused the dramatic policy shift of the past three years, and that the U.S. government will continue to remove impediments to encryption exportation. This section cautions, however, that legislation concerning encryption, like CESA, should be monitored continuously to ensure that privacy concerns are adequately addressed.

6. CESA Transmittal Letter to Congress (Sept. 16, 1999), *at* http://www.epic.org/crypto/legislation/cesa/transmittal.html [hereinafter CESA Transmittal Letter to Congress].

7. *Online Privacy Expert Rips New Clinton Internet Security Policy*, BUS. WIRE, Oct. 19, 1999, *available at* LEXIS. A prior version of CESA, previously obtained from a Department of Justice internal memorandum, was even more vehemently opposed. James P. Lucier, *Enemies of the State*, INSIGHT ON THE NEWS, Sept. 13, 1999, *available at* LEXIS. This version contained a provision that would allow government access to encryption keys, even when such keys were *not* stored with a third party. *Id.* Counsel from the Electronic Privacy Information Center ("EPIC") decried this version of CESA as "one of the scariest proposals to come out of government in a long time. This strikes at the heart of the Bill of Rights." *Id.*

8. CESA Transmittal Letter to Congress, *supra* note 6. The prospect of the bill *ever* being introduced to Congress in its current form seems highly unlikely. *See* discussion *infra* Part IV.B.

II. A BRIEF HISTORY AND EXPLANATION OF ENCRYPTION

A. What is Encryption?

Stanford Law Professor Lawrence Lessig writes with only slight exaggeration that encryption technologies are the most important technological innovations of the last millennium.[9] Encryption, or cryptography, may be understood on a basic level as scrambling information to disguise an intended communication.[10] The disguise may serve several purposes, including protecting the privacy, security, authenticity, and integrity of the communication.[11] Encryption allows a readable message—plaintext—to be transformed into an unreadable message—ciphertext—which remains incomprehensible to the recipient without a "key" to unlock the transformed message and return it to its original form.[12] An analogy between house keys and encryption keys illustrates how encryption keys function.[13] A homeowner or intended guests

9. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 35 (1999) (stating that "[c]ryptography will change everything" in social and political life).

10. The explanation of encryption offered in this Note merely aims to provide rudimentary concepts to appreciate the debate about encryption policy. The reader is forewarned that modern encryption technology is complex and involves highly technical subtleties. For a more technical explanation of encryption theory, see David B. Walker, *Privacy in the Digital Age*: *Encryption Policy–A Call for Congressional Action*, 1999 STAN. TECH. L. REV. 3, 13-20 (1999). For an explanation from the perspective of a well-known corporation that specializes in encryption products, see *RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1*, *at* http://www.rsasecurity.com/rsalabs/faq/ (last visited Jan. 3, 2001). The site offers a full index of questions and answers in a fairly objective manner and is a valuable resource in sorting through confusing topics. *See id.*

11. WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 12 (1998).

12. *Id.* at 13-14.

13. *Id.*

> The analogy with locks and keys is particularly apt in another respect. The lock and key are distinct components of a system that controls the use of doors, cabinets, cars, and other things. The lock is a moderately complex mechanical device with numerous moving parts—about two dozen in the case of a normal door lock. The key is a single piece of metal. There are, on the other hand, far fewer types of locks than cuts of keys. Most doors use one of a dozen popular brands of locks, each of which can be keyed to accept one of a million different possible keys. A lock is typically far more expensive than its key, and more expensive to replace, particularly with a lock of a different kind. Perhaps the most important distinction between locks and keys is that locks are not, in principle, secret. Locks are easily recognizable even if they do not display their brand names, and there is no reason to be concerned that people know what type of lock you use on your front door. The cut of the key, on the other hand, is a secret, and any locksmith or burglar who knows it can make a duplicate that will open the door.
>
> In exactly the same way, cryptographic systems are divided into the so-called

may enter a home through use of a house key that fits the lock on the front door and allows the keyholder to gain access, while keeping non-keyholders outside. Similarly, encryption keys allow intended readers to "unlock," and thereby understand, messages while keeping uninvited readers locked safely outside the circle of understanding.

While this Note focuses on the modern implications of encryption, the field's significant past should not be overlooked.[14] Initially, cryptography was accomplished simply through the manual substitution of one item for another to provide security in communications or information transmissions.[15] Early military communications employed this method and still comprise one of the most prevalent uses of encryption, because different factions often need to transmit messages to one another and ensure integrity.[16] With the advent of radio signals in World War I, the military required a stronger method of encryption, because messages were increasingly vulnerable to interception.[17] Cryptographers thus began to work on mechanizing encryption, a path that led to the automatic encryption systems used today.[18]

B. Modern Encryption

Just as World War I and radio signals led to a rethinking of encryption systems, the expansion of the Internet created similar demands for even more secure encryption technology.[19] Exponential advancements

> *general system* (or just *system*) and the *specific key* (or *key*). It has been a principle of cryptography for more than a century that the general system should not be regarded as secret. The keys, in contrast, must be kept secret, because anyone who is in possession of them will be able to read encrypted messages, just as anyone who is in possession of a door key can open the door.

Id. at 13 (citation omitted).

14. *See id.* at 12.

15. *Id.*

16. Indeed, a famous use of cryptography in this context allowed the United States to garner a decisive victory against the Japanese at the Battle of Midway, when naval intelligence was able to ascertain the destination of the Imperial Japanese Fleet by breaking Japan's Purple Code. Joel C. Mandelman, *Lest We Walk Into the Well: Guarding the Keys—Encrypting the Constitution: To Speak, Search & Seize in Cyberspace*, 8 ALB. L.J. SCI. & TECH. 227, 230 (1998). "Encryption, and the breaking of codes and ciphers, has been of overwhelming importance in the diplomatic and military history of the United States since the Civil War. By intercepting enemy messages, battlefield commanders learned where troops were heading and in what numbers." *Id.*

17. DIFFIE & LANDAU, *supra* note 11, at 49-50.

18. *Id.* at 50.

19. The growth of the Internet has astounded many. In November 1998, it was estimated that 140 million people around the world were connected to the Internet. U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, TOWARDS DIGITAL EQUALITY, 2ND ANNUAL REPORT 5 (1999), *available at* http://www.ecommerce.gov/ecomrce.pdf (last

in access, speed, and power have created a global interdependence unseen and—some might argue—unimagined until the past decade. Encryption's smooth and often imperceptible integration into daily life has become essential to modern day society.[20] Encryption is used to protect individual and business finance, as well as the national infrastructure that runs power grids, hospitals, and communications.[21] More notably, the explosion of e-commerce makes it difficult to recall *not* being able to buy a plane ticket online or trade stocks from one's personal computer, and many take advantage of these new conveniences.[22]

These advances come at a price, however, which must be contained through adequate security measures to protect the large, growing quantities of sensitive and private information that now move along digital channels. Recently, the fragility of Web site security became painfully clear when a hacker published thousands of credit card numbers obtained from customers of CD Universe after the company refused a ransom demand.[23] Public awareness of the vulnerability of online information has helped create a large market for strong encryption technology.[24] This new-age encryption technology, while based on the same simple substitution foundation of earlier cryptography, is now increasingly, and necessarily, complex.

The modern process by which a message is encrypted and decrypted involves complicated mathematical algorithms.[25] The strength of an

visited Jan. 19, 2001) [hereinafter TOWARDS DIGITAL EQUALITY]. This number jumped 40% to more than 200 million by September 1999, and is expected to continue to climb. *Id.*

20. Using a PIN number at an ATM is an example of encryption used by many on a daily basis. *See RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1, How is Cryptography applied?*, *at* http://www.rsasecurity.com/rsalabs/faq/1-4.html (last visited Jan. 3, 2001).

21. Kenneth P. Weinberg, *Cryptography: "Key Recovery" Shaping Cyberspace (Pragmatism and Theory)*, 5 J. INTELL. PROP. L. 667, 680 (Spring 1998).

22. Estimates in early 1998 predicted that Internet retailing would reach as high as $7 billion by the year 2000. TOWARDS DIGITAL EQUALITY, *supra* note 19, at 6. E-commerce continues to grow worldwide and the possibilities seem endless. *See id*.

23. Margaret Mannix, *High-tech card fraud goes on right behind your back*, U.S. NEWS & WORLD REP., Feb. 14, 2000, at 54, 55. Gregory Regan, a U.S. Secret Service agent involved in the financial crimes division, notes, "Credit card fraud is the bank robbery of the future," a problem only exacerbated by the Internet. *Id*. at 54.

24. *See* DIFFIE & LANDAU, *supra* note 11, at 6 (noting a researcher's estimate that the market for commercial cryptography, even though relatively new, has already surpassed that of the military).

25. The Center for Democracy and Technology ("CDT"), a non-profit public policy organization that works to promote civil liberties in the digital age, offers a fairly comprehensive glossary of cryptographic terms on its Web site. *See* Ctr. for Democracy and Tech., *Glossary of Cryptographic Terms*, *at* http://www.cdt.org/crypto/glossary.shtml (last visited Jan. 3, 2001); Mai-Trâm B. Dinh, *The U.S. Encryption Export Policy: Taking the*

encryption key is determined by how difficult it would be for a third party to break the code, which depends on the key length, measured in bits, and the complexity of the algorithm in question.[26] Bits are the digits "0" and "1" used for encoding computer data; the greater the number of bits, the greater security afforded in an encryption algorithm, because more combinations are possible, thereby making the code harder to break.[27] For example, a 40-bit key length offers more than a trillion possible combinations, a 56-bit key length permits more than 72 quadrillion combinations, and a 128-bit key length allows 3.4×10^{34} possible combinations of key sequences.[28]

The most common, and widely used, algorithm is the Digital Encryption Standard ("DES"), which has a key length of 56 bits and was developed by the federal government in the 1970s.[29] The 56-bit key length was once considered secure, but recent DES "cracking contests," sponsored by a prominent producer of encryption technology, have proven otherwise.[30] The weakness of a 56-bit key length also becomes apparent when one recognizes that by June 1999, the *minimum* strength to meet the standards of new Internet applications was 128-bit encryption.[31] Since recognizing the problem in 1997, the National Institute of Science and Technology ("NIST"), a division of the Department of Commerce, has been working to create a more powerful algorithm, known as the Advanced Encryption Standard ("AES").[32] In October 2000, NIST announced the selection of an algorithm named "Rijndael" as the proposed AES.[33]

Byte Out of the Debate, 7 MINN. J. GLOBAL TRADE 375, 379 (Summer 1998).

26. Dinh, *supra* note 25, at 379.

27. Kurt M. Saunders, *The Regulation of Internet Encryption Technologies: Separating the Wheat From the Chaff*, 17 J. MARSHALL J. COMPUTER & INFO. L. 945, 947 n.16 (Spring 1999).

28. Dinh, *supra* note 25, at 379-80.

29. Walker, *supra* note 10, at 16.

30. *Id*. RSA Data Security sponsored the contests, the most recent of which occurred in January 1999, where the algorithm was cracked in merely 23 hours. *Id*. By November 1998, because of concerns that DES was not secure, the U.S. government no longer approved its use in original form. *Id.* at 16 n.60.

31. *Immediate Need for Relaxation of Export Controls for Software and Hardware with Encryption Capabilities*: *Hearing Before the Senate Comm. on Commerce, Sci. and Transp.*, 106th Cong. 7 (1999) (statement of D. James Bidzos, Vice Chair, Security Dynamic Technologies, Inc., Parent Company of RSA Data Security, Inc., on behalf of Americans for Computer Privacy) [hereinafter Statement of D. James Bidzos].

32. Nat'l Inst. of Sci. and Tech., *Advanced Encryption Standard (AES) Development Effort*, *at* http://csrc.nist.gov/encryption/aes (last visited Jan. 19, 2001).

33. *See Commerce Department Announces Winner of Global Information Security Competition*, *at* http://www.nist.gov/public_affairs/releases/g00-176.htm (last visited Jan. 27, 2001). The AES was determined through a series of contests, in which submissions were taken from members of the global cryptographic community. A group of fifteen candidates

Assuming the rest of the development schedule proceeds as expected, AES should be completed by summer 2001.[34] In the interim, triple-DES, which requires the use of three DES keys, has become the de facto standard used by the U.S. government and other entities.[35]

Two basic types of widely available encryption systems are private ("symmetric") key systems and public ("asymmetric") key systems.[36] In a private key system, the same key is used to both encrypt and decrypt the message. Therefore, the system remains vulnerable because the key used to decrypt the information must be sent to the intended recipient of the message, leading to the risk that the key could be intercepted.[37] The key itself might also be more vulnerable to attack because it is used twice. A public key system employs two keys—a public and a private key—that are mathematically related.[38] The public key is published, thus eliminating the need to send a key through another form of communication that could be intercepted.[39] Anyone can encrypt a message using the public key, but only the intended recipient, with sole possession of the private key, can decrypt the message. For example, if Karen wants to send a confidential communication to Andy, she can look up Andy's public key, encrypt the message using the key, and then send the encrypted message to Andy. Only Andy will be able to read the message, because he holds the private key capable of decrypting the scrambled message.[40]

As illustrated by the preceding paragraphs, encryption is a highly technical field previously only of interest to a select few in the military or technological industry. Unfortunately, the complex scientific language surrounding this technology sterilizes the subject area and causes

was announced on August 20, 1998, and the final algorithm was chosen in October 2000. Rijndael was chosen "because it had the best combination of security, performance, efficiency, implementability and flexibility." *Id.*

34. *Id.*

35. DIFFIE & LANDAU, *supra* note 11, at 28.

36. Saunders, *supra* note 27, at 948.

37. *Id*. The protection of the integrity and security of keys is known as "key management." *Id*.

38. *Id*.

39. Walker, *supra* note 10, at 17. It should be noted, though, that because the private and public keys are mathematically related, the discovery of the public key can easily lead to the attack and discovery of the private key. *Id.* Therefore, robust encryption is essential. *See id.*

40. Saunders, *supra* note 27, at 948. Public key encryption may also be used as a digital signature that allows a person or a business to ensure the integrity of an electronic document. *Id.* For more information on digital signatures and their future importance for e-commerce and other applications, see Raneta Lawson Mack, Comment, *Digital Signatures, the Electronic Economy and the Protection of National Security: Some Distinctions with an Economic Difference*, 17 J. MARSHALL J. COMPUTER & INFO. L. 981 (Spring 1999).

encryption to seem a relatively benign topic. Such an assessment is dangerously naïve. With the movement of personal records and private information from wallets and locked drawers into the borderless world of cyberspace, individuals must be able to rely on new methods of security to protect their interests. Furthermore, business organizations and consumers alike must become and remain confident in the integrity of digital transactions to ensure continued growth in the area. Not surprisingly, because of the importance of encryption, the federal government, until recently, has taken a very heavy-handed approach to regulating encryption technology, which has significantly impacted the encryption debate.

III. GOVERNMENT INVOLVEMENT IN THE REGULATION OF ENCRYPTION

A. Balancing Competing Interests

As online security has become increasingly important throughout the past decade, two concerns regarding encryption regulation have divided the U.S. government: (1) the ability of American high-tech industries to compete in foreign markets; and (2) the ability of criminals and terrorists to threaten national security through the use of strong encryption devices.[41] Through a complicated combination of regulations, such as key-length export limits and license exemptions for software and equipment over those key lengths only *after* governmental review, the government has placed its domestic high-tech industry at a severe disadvantage.[42] Initially, other countries waited for the United States, the leader in strong consumer cryptography, to take action. Domestic stagnation coupled with lax restrictions by foreign governments, however, have caused U.S. industry to lag behind its competition.[43] Arguably, government regulation has impinged upon the economic growth of an industry that in 1996 had sales upwards of $1.8 billion.[44] Some critics contend that, because of U.S. restrictions, the industry has already lost more than $65 million.[45]

The government's justification for tight regulation stems from national security concerns. In the past, electronic surveillance, such as

41. *See* Walker, *supra* note 10, at 22-31; DIFFIE & LANDAU, *supra* note 11, at 77-108.

42. Christina A. Cockburn, Comment, *Where the United States Goes the Rest of the World Will Follow—Won't It?*, 21 HOUS. J. INT'L L. 491, 502-04 (Spring 1999).

43. *See id. But see* Dinh, *supra* note 25, at 390 ("Australia, Israel, Canada, China, and New Zealand boast growing encryptions industries. However, these governments generally enforce far more restrictive export controls than the United States. . . . Thus, the international encryption market is not as open as many argue.").

44. Cockburn, *supra* note 42, at 498.

45. Weinberg, *supra* note 21, at 687.

court-ordered wiretaps, has proven successful in the detection, prevention, and prosecution of crimes.[46] Based on this success, the government has attempted to limit the overall strength of encryption software so that, when an encrypted message is intercepted, the government will have the ability to decrypt it.[47] Law enforcement officials feared that continued development of strong encryption would cause them greater difficulties in remaining abreast of technological advances in a time frame conducive to preventing harm.[48] While these concerns are well founded, some compromise must be reached that effectively balances the ability of the government to protect its citizens against the high-tech industry's ability to create and market strong encryption products.

B. Governmental Regulation in the Form of Export Restrictions

No restrictions exist on the use, creation, or sale of encryption products within the United States. Exportation of encryption technology, however, has been heavily restricted.[49] Until 1996, many encryption technologies were classified as "munitions," based on the predominant military use of cryptography, and their export was forbidden under the Export Administration Regulations ("EAR"),[50] which along with the International Traffic in Arms Regulation ("ITAR"),[51] administers the Arms

46. *Security and Freedom Through Encryption (SAFE) Act: Hearing Before the Subcomm. on Courts and Intell. Prop. of the House Comm. on the Judiciary*, 106th Cong. 49 (1999) (statement of Ronald D. Lee, Assoc. Dep. Att'y Gen., Dep't of Justice).

47. *Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act: Hearing Before the Senate Comm. on Commerce, Sci., and Transp.*, 106th Cong. (1999) (statement of the Honorable James Robinson, Assistant Att'y Gen., Criminal Division, Dep't of Justice), *available at* http://www.senate.gov/~commerce/hearings/0610rob.pdf (last visited Feb. 2, 2001).

48. *Id*. Mr. Robinson also offered anecdotal evidence evincing the need for strong, but recoverable, encryption:

> I want to emphasize that this concern is not theoretical, nor is it exaggerated. Although the use of encryption is far from universal, we have already begun to encounter its harmful effects. For example, in an investigation of a multinational child pornography ring, investigators discovered sophisticated encryption used to conceal thousands of images of child pornography that were exchanged among members. Similarly, in several major computer hacker cases, the subjects have encrypted computer files, thereby concealing evidence of serious crimes. . . . Finally criminal use of encryption is increasingly international—the United Kingdom recently reported that in 1996 it seized encrypted files from a Northern Irish terrorist group concerning terrorist targets such as police officers and politicians. In that case, law enforcement was able to read the data, but only after considerable effort.

Id.

49. Saunders, *supra* note 27, at 949.

50. 15 C.F.R. pts. 730-99 (2000).

51. 22 C.F.R. pts. 120-30 (2000).

Export Control Act ("AECA")[52] through the State Department.[53] Encryption technology is also considered a dual-use technology, because it is used by both military and civilians.[54] In fact, the growing civilian use of encryption might arguably be more important than its military use.[55]

On November 15, 1996, former President Clinton signed an Executive Order that transferred regulation of all encryption technologies, except those developed solely for military use, to the Commerce Department.[56] The action arguably benefited hopeful exporters of encryption technology who anticipated that the Commerce Department's staff would expedite license grants.[57] Under State Department regulation, it could take a significant amount of time for a company to obtain an export license.[58] The 1996 transfer order was followed by an announcement in September 1998 that the government would allow the export of increased bit-length products and relief for certain industry groups, including U.S. subsidiaries and insurance companies.[59] Reform efforts reached their apex with the January 12, 2000 announcement allowing export of strong encryption technology with few exceptions.[60] The government's laissez-faire attitude continued in July 2000, when President Clinton's Chief of Staff, John Podesta, announced that U.S. companies could export *any* encryption products without a license to *any* end-user in the fifteen nations of the European Union, as well as Australia, Norway, the Czech Republic, Hungary, Poland, Japan, New Zealand, and Switzerland.[61] This

52. 22 U.S.C. § 2778 (1994 & Supp. IV 1998).

53. Saunders, *supra* note 27, at 950.

54. *Id*.

55. *See supra* note 22 and accompanying text.

56. Exec. Order No. 13,026, 3 C.F.R. 228 (1996).

57. Stewart A. Baker & Peter Lichtenbaum, *Cutting Red Tape on Encryption*, J. COM., Sept. 27, 1996, at 9A.

58. *See* Walker, *supra* note 10, at 25-26.

59. CDT, *An Overview of Clinton Administration Encryption Policy Initiatives*, *at* http://www.cdt.org/crypto/admin/initiatives.shtml (last visited Jan. 19, 2001) [hereinafter *Overview of Encryption Policy*]. Because businesses feared that corporate secrets would be vulnerable to attack, the Clinton Administration allowed the use of unlimited encryption for certain U.S. subsidiaries, companies in the health and medical fields, online merchants, and insurance companies. Cockburn, *supra* note 42, at 508.

60. For example, the bit length of encryption keys has been allowed to increase over time. Similarly, while the Clinton Administration once strongly advocated mandatory key escrow, it was forced to back away from this stance, possibly because of the negative reaction to Clipper Chip. *See infra* Part III.B.1.

61. Press Release, Office of the White House Press Secretary, Administration Updates Encryption Export Policy (July 17, 2000), *available at* http://www.pub.whitehouse.gov/. The White House added: "The steps announced today continue our policy to serve the full range of national interests: promote electronic commerce, support law enforcement and national security, protect privacy, and maintain U.S. industry leadership in security

announcement eliminated technical review and the resulting delay in overseas sales.[62]

1. Domestic Executive Initiatives

Prior to the January 12, 2000 liberalization of encryption export policies, the Clinton Administration had initiated a number of domestic policies regarding encryption. Clinton was the first president forced to face the strong and undeniable influence of the Internet on the global stage. As such, the past eight years have been an experimental time for encryption and Internet policy alike, and President George W. Bush will face the challenge of implementing policy that found its genesis during the prior administration.[63]

During his presidency, Clinton made enemies of privacy groups and members of the high-tech industry with initiatives such as the 1993 proposal of the ill-fated "Clipper Chip,"[64] a physical chip that would have allowed the government to access encrypted information.[65] The algorithm used for the Clipper Chip ("Clipper") was developed by the National Security Agency ("NSA") and known as "Skipjack." Because the NSA classified the Skipjack algorithm, it was not possible to make judgments about its strength.[66] Detractors complained that electronic security was too important to allow the government to classify algorithms without public scrutiny.[67] Three more Clipper proposals followed, the last being Clipper 3.1.1, which, as proposed, continued restrictions on exported encryption technology to enforce mandatory key escrow.[68]

---

technologies." *Id*.

62. *Id*.

63. Though currently it is unclear exactly how the Bush Administration will tackle issues like encryption technology, an article by then-candidate Bush offers some insight:

> Our current technology export system is broken. Our best companies cannot sell some products abroad—even when foreign competitors sell equivalent technology. I will safeguard military technology and let Americans sell what is already widely available. I will lead efforts to free the sale and export of American computers, as well as other high-tech goods, including encryption software.

George W. Bush, *Technology and prosperity: Let dreams flourish* COMPUTERWORLD, August 9, 1999, at 30, *available at* LEXIS, News Group File, Most Recent Two Years.

64. EPIC, *The Clipper Chip*, *at* http://www.epic.org/crypto/clipper/ (last visited Jan. 3, 2001) [hereinafter *The Clipper Chip*].

65. *Id*.

66. *Id.*

67. George Leopold, *Report: Dump Clipper, Open Encryption Debate*, ELEC. ENG'G TIMES, July 4, 1994, at 4. "The Clinton Administration should drop its Clipper key-escrow proposal and launch a public review of U.S. encryption policy to better balance privacy concerns with law enforcement and national security issues, a report by a panel of encryption experts, including Clipper supporters, concludes." *Id.*

68. *Overview of Encryption Policy*, *supra* note 59. This site also offers information on

Arguably, the promotion of mandatory key escrow was the most significant aspect of the Clipper Chip proposals.[69] Key escrow is a process that requires a copy of decryption keys, similar to a spare set of house keys, to be placed into escrow with a third party, known as a Trusted Third Party ("TTP").[70] Another example of a TTP is a Certificate Authority ("CA"), a public or private body that can issue digital certificates of authenticity in e-commerce situations where one party wants to verify the ownership of an individual's public key.[71] Stored keys may be accessed if the original keyholder loses or forgets the information.[72] Without a third-party recovery system, the message could remain encrypted indefinitely, causing great delay and inconvenience.[73] Despite the innocuous uses of key escrow, also known as back-door software,[74] the process often has been insidiously associated with the ability of government to decode messages under the guise of law enforcement and national security.[75]

The 1993 introduction of Clipper, and the three similar proposals that followed, illustrates but one route attempted by the Clinton Administration to advocate development and use of key escrow. In what could be interpreted as an attempt to force the high-tech industry to submit to governmental desires, the Clinton Administration offered to allow export of encryption software to other countries, provided that a spare set of keys was turned over to a government-approved TTP, which could then release the keys during an investigation.[76] The high-tech industry and others argued forcefully that such action notably reduced the viability of the software for export. Foreign consumers, aware of the U.S. government access, understandably balked at the potential of exposing private or business

Clipper II, proposed in 1995, and Clipper III, proposed in the summer of 1996. *Id*.

69. *See The Clipper Chip*, *supra* note 64.

70. Dinh, *supra* note 25, at 379-81. Examples of TTPs, also called key recovery agents, are commercial or governmental entities which meet some level of trustworthiness. *Id.* at 380 n.41. *See also* Walker, *supra* note 10, at 20.

71. Walker, *supra* note 10, at 20.

72. *RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1, What is key recovery?*, *at* http://www.rsasecurity.com/rsalabs/faq/7-12.html (last visited Jan. 3, 2001).

73. *Id*.

74. *Id*.

75. DIFFIE & LANDAU, *supra* note 11, at 7.

> The effect is very much like that of the little keyhole in the back of the combination locks used on lockers of schoolchildren. The children open the locks with the combinations, which are supposed to keep other children out, but the teachers can always open the lockers by using the key.

Id.

76. EPIC, *Key Escrow*, *at* http://www.epic.org/crypto/ key_escrow/ (last visited Jan. 19, 2001) [hereinafter *Key Escrow*].

documents to the U.S. government.[77] Therefore, the software industry adamantly opposed this regulation and restriction on trade.[78]

2. International Executive Initiatives

Facing domestic resistance to mandatory key escrow, the Clinton Administration attempted to pressure other countries to support restrictions on the export of encryption software over a certain key length.[79] Despite lobbying efforts by the White House, on March 27, 1997, the Organization for Economic Cooperation and Development ("OECD") adopted cryptography guidelines that did *not* advocate a strong position in favor of key escrow.[80] Also frustrating was the October 8, 1997 European Union ("EU") publication of a draft paper adopting market forces and self-regulation of industry as its official stance toward encryption—a view the Clinton Administration strongly opposed.[81] Finally, the Administration's mandatory key escrow policy suffered a lethal hit when the Wassenaar Arrangement group, an agreement between thirty-three industrialized countries to restrict exportation of dual-use technologies to certain countries, rejected key escrow in 1998.[82]

It is now apparent that the strength of encryption products available worldwide cannot be controlled unilaterally by the United States. Indeed, it makes little sense to restrict domestic companies from exporting encryption

77. Mack, *supra* note 40, at 995. "Opponents argue that backdoor access will be a strong disincentive for non-U.S. companies to purchase the software and will only increase the foreign competitive advantage by providing more business for software companies outside the U.S. that do not impose such a requirement." *Id.*

78. Rutrell Yasin, *Senators Pledge to Push Encryption Reform*, INTERNETWEEK, June 22, 1998, *available at* LEXIS. Leading computer executives, including then-Microsoft CEO Bill Gates, met with former Attorney General Janet Reno and FBI Director Louis Freeh to work out an amicable solution in June 1998, but neither side would agree to change its position. *Id.*

79. EPIC, *Cryptography and Liberty 2000: An International Survey of Encryption Policy*, *at* http://www2.epic.org/reports/crypto2000/ overview.html#Heading9 (last visited Jan. 19, 2001) [hereinafter *Cryptography and Liberty*]. *See also* Cockburn, *supra* note 42, at 520-25.

80. Cockburn, *supra* note 42, at 521. Despite this apparent victory for key escrow opponents, the Clinton Administration's push to the organization about the benefits of key escrow did make some countries more sympathetic than they had previously been to the U.S. argument. *Id.*

81. Mack, *supra* note 40, at 995.

82. *Cryptography and Liberty*, *supra* note 79. Some might argue that the worst blow, though, was dealt by a November 1996 memorandum from William A. Reinsch, the Commerce Department's Under Secretary for Export Administration, which admitted to the inferiority of Clinton's favored key escrow technology. Mem. from William A. Reinsch, The Under Secretary for Export Administration, U.S. Dep't of Comm., to Deputies Subgroup on Cryptography (Nov. 25, 1996), *available at* http://www.epic.org/crypto/key_escrow/reinsch_memo.html.

technology over a certain bit length when such technology is readily available in other markets. With the ability to download information from the Internet, a criminal or terrorist could easily obtain robust encryption technology from foreign software companies online and violate no law. In such a scenario, the government cannot decrypt criminal communications, and limiting the strength of the encryption products that U.S. companies can export does not address the problem. An artificially imposed limit on the strength of exported encryption technology only serves to make the American software industry, which accounts for seventy percent of the world market, less competitive where it once had a decisive edge.[83] In addition, the recent growth in the software industry has produced many new jobs in the United States, as well as billions of dollars in tax revenue.[84] To stifle such progress through regulations on encryption technology is unnecessary and ineffective.

C. Legislative Response

In the face of executive initiatives, Congress grew increasingly vocal regarding the proper response of the legislature to encryption technology. Since 1997, a variety of legislation has been promulgated.[85] Arguably, the Security and Freedom Through Encryption ("SAFE") Act, introduced by Representative Bob Goodlatte (R-VA) and Representative Zoë Lofgren (D-CA), gathered the most momentum.[86] SAFE's intent was to protect domestic use of encryption, as well as to ease export controls dramatically.[87] SAFE prohibited mandatory key recovery, allowed the export of available software and hardware if a product of similar strength was already on the market, and created criminal penalties for using encryption to conceal a crime.[88] The bill garnered a great deal of bipartisan

83. Statement of D. James Bidzos, *supra* note 31, at 5.

84. *Id*.

85. Other proposed pieces of legislation which are beyond the scope of this Note but trace congressional interest in the encryption arena, include Promote Reliable On-Line Transactions to Encourage Commerce and Trade ("PROTECT") Act of 1999, sponsored by Sen. John McCain (R-AZ). S. 798, 106th Cong. (1999). The bill aimed to promote e-commerce through encouraging the use of encryption in interstate commerce, consistent with national security objectives. *Id*. *See also* Encryption for the National Interest Act, H.R. 2616, 106th Cong. (1999); Secure Public Networks Act, S. 909, 105th Cong. (1997); Promotion of Commerce On-Line in the Digital Age, S. 377, 105th Cong. (1997); Encrypted Communications Privacy Act of 1997, S. 376, 105th Cong. (1997).

86. H.R. 850, 106th Cong. (1999).

87. CDT, *SAFE H.R. 850, at* http://www.cdt.org/ crypto/legis_106/SAFE/ (last visited Jan. 3, 2001).

88. *Id*.

support and more than 250 co-sponsors.[89] After the bill's circulation through a variety of committees, its proponents were optimistic that the legislation could be passed in 2000 because of its support in Congress, as well as from industry, privacy advocates, and consumer groups.[90] At a hearing before the House Judiciary Committee, several industry members testified in support of the bill and the immediate need for relaxation of encryption policy.[91] SAFE explicitly rejected the Clinton Administration's desire for mandatory key escrow, and would have allowed U.S. industry the ability to contend with foreign competitors.[92] In advancing legislation like SAFE, Congress pushed the Clinton Administration to accept the emergence of a global interconnection that the U.S. cannot exclusively control.

With the new regulations announced on January 12, 2000, however, the driving force behind SAFE diminished, and the issue now appears to be moot.[93] Representative Lofgren said of the change in policy: "It's not perfect, but it's not bad. . . . Much of what we hoped to achieve through SAFE has been achieved through these regulations."[94] She also said it would be a mistake to continue to push the bill because much had been achieved through the new regulations.[95] Representative Goodlatte was more guarded in his comments, stating that lawmakers would carefully watch future actions by the Administration, and take up SAFE again if "the regulations do not allow American companies to fully compete in the

89. *Id.*

90. Cockburn, *supra* note 42, at 515.

91. *Security and Freedom Through Encryption (Safe) Act: Hearing on H.R. 850 Before the Subcomm. on Courts and Intell. Prop. of the House Comm. on the Judiciary*, 106th Cong. 137 (1999) (testimony of Dave McCurdy, President of the Electronic Industries Alliance) Electronic Industries Alliance is an alliance of trade associations with more than 2000 member companies. *Id. See also id.* at 74 (testimony of Thomas Parenty, Director of Data and Communications Security for Sybase, Inc.). Parenty is responsible for security-related product development at one of the top ten largest software companies in the world. *Id*. Parenty has also worked at the NSA, and was testifying on behalf of the Business Software Alliance ("BSA"). *Id*. He made three main points in his testimony before the Subcommittee:

> Widespread deployment of encryption is not only desirable, it is critical; America's export policy should promote widespread deployment of products with encryption capabilities in the worldwide market; and BSA strongly supports the SAFE Act because it provides freedom for Americans to use and sell any encryption domestically and provides greatly needed export control relief.

Id. at 75.

92. *Id.*

93. *Reducing US Crypto Export Rules*, WIRED NEWS (Jan. 13, 2000), *at* http://www.wired.com/news/business/0,1367,33625,00.html.

94. Schwartz, *supra* note 4.

95. *Id*.

global marketplace."[96] For the moment, legislative action has stalled and will await further catalysis by the Bush Administration.

IV. WHITE HOUSE ENCRYPTION POLICY ANNOUNCEMENT OF 1999: NEW EXPORT REGULATIONS AND CESA

The September proposal contained both encryption regulation and proposed legislation, but the proposed export regulations garnered the majority of media and political attention.[97] The two-part announcement included (1) the relaxation of export regulations, and (2) CESA. By including CESA in the announcement, the government made clear that it had not abandoned its advocacy of recoverable (key escrow) encryption technology. CESA would ensure law enforcement access to decryption keys stored with third parties. This Note will now discuss each part of the September proposal in turn.

A. The New Export Regulations

Per its promise in the September proposal, the BXA released a draft of the new encryption export regulations in November 1999.[98] Despite the regulations' lessened controls on retail encryption, high-tech representatives and privacy groups protested that the results fell short of promises made in September.[99] Complaints arose regarding the complexity of the regulations, but industry representatives did praise the Administration's decision to give source code the same treatment as other commercial products.[100] William A. Reinsch, the Under Secretary of Commerce who headed the BXA, stated that the regulations were a "work in progress" and were offered to the public in order to solicit input and "take their criticisms to heart."[101]

96. *Reducing US Crypto Export Rules*, *supra* note 93.

97. *See* Jerry Seper, *Clinton Seeks to Step Up Computer Code Exports*, WASH. TIMES, Sept. 17, 1999, at A4.

98. *See* Jeri Clausing, *Administration Releases Draft of Encryption Export Rules* (Nov. 23, 1999), *at* http://www.nytime.com/library/tech/99/11/cyber/articles/24code.html.

99. *Id*. Stewart Baker, partner at the law firm of Steptoe & Johnson in Washington, D.C., felt that the regulations were much better than the scheme under which the U.S. had operated, and felt that any complaining was inappropriate. "[T]here's a part of me that wants to say, 'You've been upgraded from a prop plane to a Concorde and now you're going to complain that you didn't get a window seat?'" *Id*.

100. *Id*. Source code is a written version of software that allows anyone trained in the computer language to interpret and understand how the program is constructed. *Id*.

101. *Id*. Reinsch also cynically noted:

> We assumed nobody was going to be happy because they never are—My objective was to put forth a good faith effort that reflects what was said in September, a good faith effort to keep it simple. But we felt at this point in the process the smartest thing to do was to get the paper out and get comment so we

The finalized regulations released in January 2000 answered some of the concerns voiced in November, but still drew fire based on their highly complicated nature.[102] The new regulations substantially loosened restrictions, and virtually all encryption programs on the retail market can now be sold overseas after a "one-time" government review.[103] American companies also now have the ability to export encryption products of *any* key length to commercial firms and individual consumers without the license that was previously required.[104] Further, U.S. companies may export any encryption item to foreign subsidiaries through streamlined requirements, and foreign employees no longer need export licenses to work on encryption.[105] The longstanding prohibition on exporting encryption software to states supporting terrorism—Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria—still remains in effect.[106] Former Commerce Secretary William M. Daley stated that "[t]his policy helps business and promotes e-commerce by adjusting our regulations to marketplace realities that U.S companies face when they try to sell their products overseas."[107]

The January 2000 regulations represented a good-faith effort by the BXA and the Clinton Administration to answer industry and individual concerns, but problems remained. First, the one-time technical review of encryption products prior to export still allowed the government access to the encryption process prior to sale, which made the products unattractive to foreign consumers as well as privacy proponents.[108] Second, the highly technical nature of the restrictions forced anyone desiring to export encryption technology to seek the advice of an attorney skilled in the area–an expensive proposition.[109] While retaining advice of experienced counsel may not be a difficult task for a large corporation with adequate financial

could go back to the drawing board.

Id.

102. *See* Schwartz, *supra* note 4.

103. Press Release, Department of Commerce, Commerce Announces Streamlined Encryption Export Regulations (Jan. 12, 2000), *available at* http://204.193.246.62/public.nsf/docs/60D6B47456BB389F852568640078B6C0.

104. *See id.*

105. *Id*.

106. *Id*.

107. *Id.*

108. *See* Press Release, EPIC, ACLU, EFF, Civil Liberties Groups Say New Encryption Export Regulations Still Have Serious Constitutional Deficiencies (Jan. 13, 2000), *available at* http://www.epic.org/crypto/export_controls/joint_release_1_00.html.

109. Sanger & Clausing, *supra* note 2. Alan Davidson, an attorney for the CDT notes that "[t]he good news is that consumers all over the world are going to have access to much stronger encryption. The bad news is that if you want to send encryption out of the country, you have to hire a lawyer to do it. These regulations are very complicated." *Id.*

resources, the young entrepreneur or small business is not similarly situated, and, thus, stands at a disadvantage.[110] Because individuals who have grown up in the information age have unique perspectives and abilities, any economically restrictive policy hampers the success and motivation of those with limited resources, and thus advancement in general.[111] Third, licenses were still required if foreign governments purchased products.[112] Reinsch stated that this could apply to foreign companies partially owned by governments—a significant restriction because many foreign governments own telecommunication providers and other companies.[113] Finally, the Center for Democracy and Technology ("CDT") argued that the regulations did not address First Amendment concerns by failing to "exempt researchers from sharing their codes with foreign counterparts . . . [therefore causing] researchers . . . to ask for permission before they exchange ideas with people outside of the United States."[114] The CDT argued that forcing researchers to seek permission from the government before exchanging ideas with foreign researchers functions as a prior restraint in violation of the First Amendment. The Sixth Circuit recently addressed the issue and found that the First Amendment protects computer source code, but it remanded the case to resolve whether national security interests outweigh the interests in the open exchange of encryption code.[115]

110. Schwartz, *supra* note 4.

111. Also noteworthy is that small businesses likely will be adversely affected by not using encryption for consumer protection as their larger counterparts may. Although a significant number of small businesses do use the Internet (28% of companies with less than 20 employees, 54% of companies with between 20 and 99 employees, and 62% of companies with between 199 and 499 employees), their interactions usually amount to nothing more than online brochures. TOWARDS DIGITAL EQUALITY, *supra* note 19, at 25. The reasons for this are many, but lack of knowledge about high technology, such as encryption, is significant. *Id.* at 26. This will not only make small businesses less competitive, but it soon may make them obsolete as e-commerce develops. Therefore, the technical new regulations may stand as an additional barrier to true growth and utilization by small private-sector businesses.

112. Sanger & Clausing, *supra* note 2.

113. *Id*.

114. *Id*. These comments were offered by Alan Davidson, an attorney for the CDT. *Id.* The intersection of First Amendment issues and the encryption debate are outside the scope of this Note, but have received increasing attention over the last few years, especially in regard to recent court cases including *Bernstein v. United States Dept. of State*, 974 F. Supp. 1288 (N.D. Cal. 1997). Bernstein, a mathematician, argued that the government's restriction on his ability to publish encryption research on the Web operated as a prior restraint, was vague and overbroad, and impinged on his right to freedom of association. Mack, *supra* note 40, at 990. The court found that encryption could qualify as speech protected under the First Amendment. *Id*. For more information with regard to *Bernstein*, see http://www.eff.org/bernstein/ (last visited Jan. 20, 2001).

115. Junger v. Daley, 209 F.3d 481, 482 (6th Cir. 2000).

Some concerns about the January 2000 announcement were answered by the July 2000 statement doing away with the license requirement for the EU and other specified countries.[116] Despite this attempted clarification, fear of governmental access to encrypted information is still relevant, especially in light of CESA and future legislation that may develop.

B. CESA: Implications and Probability of Passage

Along with the proposed liberalization of export regulations announced in September 1999, the Clinton Administration also submitted CESA for transmittal to Congress. CESA was drafted "[t]o protect the privacy, security and safety of the people of the United States through support for the widespread use of encryption, protection of the security of cryptographic keys, and facilitation of access to the plaintext of data for legitimate law enforcement purposes."[117]

Through CESA, the government renewed its support for key escrow and governmental access to decryption keys, the policy heavily criticized when embodied in the Clipper Chip.[118] The privacy concerns raised by activist groups to the three Clipper proposals still bear relevance to CESA, but they have been overshadowed to a certain extent by jubilant industry reaction to the loosened export regulations. Congress took no action on CESA during Clinton's final term in office, and, indeed, the chances of CESA ever being introduced in Congress are minimal.[119] Recent history, however, suggests that failed executive action on key escrow does not mean the end of the policy's political life. Further, because the impetus behind key escrow derives from national security concerns, the tension will certainly survive into the Bush Administration. Therefore, even if CESA itself never reaches Capitol Hill, careful attention should be paid to prepare for critical analysis of future legislation raising similar concerns.

116. BXA, *U.S. Updates Encryption Export Rules to European Union and Other Trading Partners* (Oct. 18, 2000), *available at* http://www.bxa.doc.gov/press/2000/EncryptionRules UpdatedOct2K.html.

117. The White House, *The Cyberspace Electronic Security Act of 1999* (Sept. 16, 1999), *available at* http://www.epic.org/crypto/legislation/cesa/bill_text.html.

118. *See infra* Part III.B.

119. A staff member at the House Subcommittee on Telecommunications offered a succinct opinion on CESA: "I don't see the bill going anywhere." Telephone interview by the Author (Feb. 3, 2000). The staff member noted that if CESA were ever introduced in the House or Senate, it would have to be "by request," because no member of the House or Senate would want his or her name attached to the bill in its current form.

1. Three Bundles of Issues: The Main Provisions of the CESA

The provisions of CESA are all too familiar. Reminiscent of Clipper, CESA was another attempt by the government, through law enforcement, to gain access to decryption keys held in key escrow.[120] Commentators contend that CESA responds to the perceived major obstacle to acceptance of key escrow—government agencies serving as TTPs.[121] Currently, no federal statutory protection exists for the privacy of decryption keys already held by TTPs or CAs, and CESA responds to security concerns by addressing "both the legitimate and unlawful uses of cryptography, [and by] building a legal infrastructure for these emerging issues."[122] In announcing CESA, the White House reassured the public that the bill does not regulate domestic development of encryption and "Americans will remain free to use *any* encryption system" they desire.[123]

CESA effectively may be divided into three bundles of issues, though this Note will address only one in detail. First, the proposal authorizes funding of $80 million over four years for the creation of the FBI's Technical Support Center to serve as the central resource for law enforcement at all levels to respond to the growing use of encryption by criminals and terrorists.[124] Second, the proposal deals with law enforcement's ability to gain access to decryption keys stored with third parties, and creates some privacy protection for decryption keys held by TTPs or CAs.[125] Finally, CESA addresses concerns that law enforcement investigations could potentially uncover trade secrets leading to litigation and liability.[126]

If CESA is enacted—again an unlikely proposition—its $80 million appropriation over four years to fund the proposed FBI support center does not raise much concern.[127] This figure is not outrageous considering the highly technical nature of encryption and the cost of the equipment needed for research in this area. In fact, with the rise in computer crime, certainly more funds need to be earmarked for law enforcement agencies to be able to protect the public. As such, the monetary appropriation does not

120. *See supra* Part III.B.

121. *See Key Escrow*, *supra* note 76, at *1.

122. The White House, *Analysis: The Cyberspace Electronic Security Act of 1999* (Sept. 13, 1999), *at* http://www.epic.org/crypto/legislation/cesa/analysis.html.

123. The White House, *Fact Sheet: The Cyberspace Electronic Security Act of 1999 (CESA)*, 1999 WL 721386 (White House) (emphasis added).

124. *Id*.

125. *Id*.

126. *Id*.

127. *See The Cyberspace Electronic Security Act of 1999*, *supra* note 117, § 207.

engender debate and, therefore, receives no further discussion in this Note.[128]

Regarding the second bundle of issues addressed by CESA, section 2711 pertains to "[d]isclosure or use of stored recovery information and customer information by recovery agents; notification of storage location,"[129] stating that a recovery agent "shall not disclose stored recovery information; use stored material to decrypt data or communications; or disclose any other information or record that identifies a person or entity for whom the recovery agent holds or has held stored recovery information" unless the third party has permission or a court order.[130] Violators of this section would be subject to fines or imprisonment of up to one year.[131] This section addresses the safety concerns associated with storing decryption keys with TTPs; despite protections offered in the provision, however, it allows law enforcement to gain access to decryption keys—and hence plaintext—without disclosure to the subject of the investigation for ninety days or longer.[132]

Section 2712 further explains how and when a governmental agency may compel disclosure of decryption keys. Disclosure may be compelled by a warrant, any process to compel disclosure under federal or state law, a court order as detailed in section 2712 (b), or an investigative or law enforcement officer's reasonable determination that an emergency situation exists.[133] Subpart (a) also allows the federal government to require the use of stored information for the benefit of a foreign government, which raises serious concerns about how foreign governments could exploit this provision.[134] A court would issue an order for disclosure upon a finding, using specific facts, that the use of the recovery keys is "reasonably necessary" to access the information, that the access is otherwise lawful, that the government will access the information within a reasonable time after getting the keys, and that there is no privacy interest in decrypted information.[135]

The question whether an entity retains a privacy interest in decryption keys stored with a third party raises serious concerns. The Justice Department has suggested that any time decryption keys are stored with a third party the storer no longer has a privacy interest in any information

128. The section pertaining to trade secrets also lies outside the scope of this Note.
129. *The Cyberspace Electronic Security Act of 1999*, *supra* note 117, § 2711.
130. *Id.* §§ 2711(a)(1)(A)-(B), (b)(1)(A)(ii).
131. *Id.* § 2711(e).
132. *Id*. § 2711(b)(2)(d).
133. *Id*. § 2712(a)(1)-(4).
134. *Id*. § 2712(a).
135. *Id.* § 2712(b)(1)-(4).

encrypted with the recoverable key.[136] Additionally, while section 2712(c) forces the government to notify the person whose decryption keys have been accessed within ninety days after decrypting the information, this time frame may be extended indefinitely on an ex parte showing of good cause—again, an ambiguous standard.[137] Unlike the contemporaneous notice the subject of an investigation receives when law enforcement searches a house or office, it is possible an individual would *never* realize the government was decrypting and reading confidential communications.

2. Criticisms of CESA

The CDT, an online privacy group that monitors encryption policy on its Web site, offered its own analysis of CESA when it was released. The group highlighted deficiencies in the proposed legislation and expressed concerns that the relaxation of export regulations may have been an anticipatory quid pro quo for industry acceptance of key escrow.[138] A policy analyst at the CDT, Lusan Chan, speculated that, because the government finally realized that export restrictions were not a viable option, it had to shift gears to ensure governmental access, "[n]ow that they realize . . . [key escrow in] the marketplace has become outdated, they are focusing on law enforcement access. We are concerned they are using this concession as a way to expand current law enforcement activity."[139] Indeed, after the January and July liberalization, the Clinton Administration might have felt, or expected, that industry and privacy groups would be more willing to accept CESA or similar legislation. The CDT also criticized the proposal for permitting foreign governments to gain access to recovery keys, as well as for allowing any federal law enforcement officer to demand a decryption key from a TTP or CA when the officer determines that an emergency exists—thereby cutting out the judicial intermediary.[140]

The largest concern raised by CESA, however, is its potential Fourth Amendment deficiencies. CESA only requires that law enforcement prove it is "reasonably necessary" to gain access to decryption keys, as opposed to meeting the more stringent "probable cause" requirement of the Fourth

136. CDT, *Initial CDT Analysis of Clinton Administration's Proposed Cyberspace Electronic Security Act (CESA): Standards for Government Access to Decryption Keys* (Sep. 23, 1999), *at* http://www.cdt.org/crypto/ CESA/cdtcesaanalysis.shtml.

137. *The Cyberspace Electronic Security Act of 1999*, *supra* note 117, § 2112(c).

138. *See* Ann Harrison, *Clinton Eases Crypto Export Ban*, COMPUTERWORLD, Sept. 20, 1999, *available at* LEXIS-NEXIS.

139. *Id*.

140. CDT, *Initial CDT Analysis of the Clinton Administration's Proposed Cyberspace Electronic Security Act (CESA): Standards for Government Access to Decryption Keys* (Sept. 23, 1999), *at* http://www.cdt.org/crypto/CESA/ cdtcesaanalysis.shtml.

Amendment.[141] Additionally, the Fourth Amendment requires the government to obtain a search warrant for an original location, and if clues from that search uncover information leading to a different location, officers must return to court and obtain another warrant.[142] Such is not the case when encrypted information is involved. For example, under CESA, a federal agent could gain access to decryption keys by "a finding of no constitutional privacy interest in the plaintext," even though she does not know what the plaintext will reveal.[143] Therefore, CESA allows seizure of decryption keys from a TTP or CA as well as the seizure of plaintext relating to the subject of the investigation—two searches for the price of one.[144]

While CESA does not require individuals or companies to store decryption keys with third parties,[145] as the use of encryption increases, more and more entities *will* store decryption keys with third parties, and thus potentially sacrifice their privacy interest in the data revealed. In a press briefing after the September proposal, Peter Swire, Chief Counsel for Privacy at OMB, invoked conservative scare tactics encouraging key escrow, stating, "Think of your bank ATM card. What would it be like if you forgot your password and could not obtain access to the money in your account. That is precisely what can happen with strong encryption. If you lose the password, then all the encrypted material is scrambled forever and lost."[146] The fate of CESA is dim, especially as more constituents realize the importance of the issue and the far-reaching implications of allowing the government access to recovery keys. Nevertheless, public consciousness of inroads into online privacy is essential, especially as a

141. *Id*.

142. *Id*.

143. *Id*.

144. *See id.*

145. Press Briefing by Administration Officials on Encryption, Sept. 16, 1999, *available at* 1999 WL 722459 (White House). When speaking at the briefing, OMB Chief Counselor for Privacy Peter Swire was quick to point out what CESA would not do:

> CESA does not require anyone to use key escrow, nor does it regulate how key escrow might develop in the private sector. The only effect of CESA on key escrow is to provide privacy assurances for those who freely choose to give their backups of key information to others. Some information stored outside of your home deserves to be carefully protected.

Id. at *8.

However, the government may protest too much. It certainly could be that in a few years, because of the amount of encryption required for effective e-commerce and secure online business transactions, people may not realize the present implications of passing such a law.

146. *Id*. at *7.

new administration assumes power.

V. WHY THE SHIFT, AND WILL IT CONTINUE?

Many have questioned why the Clinton Administration altered its U.S. encryption policy so drastically from the original announcement of the Clipper Chip in 1993. Various reasons are offered, the most obvious and accurate being the recognition of global marketplace realities and the inability of the United States to stem foreign creation of robust encryption. Because anyone with a PC and an Internet connection can download strong encryption products, the U.S. restriction on exportation of strong key-length products had little effect on the dissemination of such products globally. The old policy simply was unrealistic, which harmed the domestic encryption industry through lost revenue and opportunity for expansion.

Other reasons for the shift include pressure from powerful industry groups to loosen export restrictions. The Clinton Administration described its approach to Internet policy as an area in which the private sector should lead—a characterization undermined by unilateral government regulation.[147] Indeed, Silicon Valley has been so irritated with governmental regulation in this area, that even after the export regulations were announced in January 2000, one Washington, D.C., attorney noted that, "the Valley is only going to be satisfied when the director of the [NSA] crawls across the Bay Bridge to apologize for controls."[148] Additionally, the dramatic change in policy was linked to Al Gore's unsuccessful run for the 2000 presidency, with reports circulated that his office was flooded by complaints about the previous restrictions, and hints that if Gore wanted support from the high-tech industry, change had to occur.[149]

Progress has been made in the past two years, but the government must be monitored and regulations governing the exportation of encryption products should be further simplified. The complexity of the January 2000 regulations was simplified somewhat in July, but even after the modification, the European Commission released trade barrier reports in August, determining that the U.S. encryption regime still inhibited trade and the growth of e-commerce.[150] Additionally, as the amount of information stored online continues to grow exponentially, key escrow will

147. TOWARDS DIGITAL EQUALITY, *supra* note 19, at iii.

148. Sanger & Clausing, *supra* note 2.

149. *Id.* Gore's supporters in Silicon Valley became angry over the restrictions placed on export. *Id.*

150. *See EC Report Raises Concerns on U.S. Satellite Licensing*, COMM. DAILY, Aug. 2, 2000, at 6.

be a requisite of living and working in the new millennium. A law passed now forcing TTPs or CAs to release encryption keys to law enforcement upon request will have more effect in the future than the present, as more people will store encryption keys with a third party. Careful attention must be focused on these issues.

VI. CONCLUSION

Every cliché that has been bandied about in the past five years—the information superhighway, the technological revolution, the information age—is literally true, even if overused. Encryption technology stands at the vanguard of further advancement in the areas of e-commerce, online retailing, and the creation of a secure interconnected world. By leveling the playing field with foreign competitors, the recent relaxation of encryption regulations will certainly be a boon to the U.S. high-tech industry. Still, a critical eye must remain on further U.S. encryption policy development, especially as the Bush Administration begins to implement its agenda. Privacy concerns based on information sent over the Internet are real and growing. Future legislation similar to CESA must be evaluated for any Fourth Amendment deficiencies. Such evaluation is necessary in the world as it will be—a world where the most intimate information is not stored in a safe, but in an encrypted file on a network accessible to anyone with the right key.