UIC Law Review

Volume 29 | Issue 2 Article 8

Winter 1996

The Clipper Chip Proposal: Deciphering the Unfounded Fears That Are Wrongfully Derailing Its Implementation, 29 J. Marshall L. Rev. 475 (1996)

Howard S. Dakoff

NOTES

THE CLIPPER CHIP PROPOSAL: DECIPHERING THE UNFOUNDED FEARS THAT ARE WRONGFULLY DERAILING ITS IMPLEMENTATION

INTRODUCTION

Improvements in technology have reduced law enforcement's ability to conduct electronic surveillance of criminal activity.[1] Rather than rely on telephones to communicate with their accomplices, criminals may increasingly use computers to perpetrate crimes.[2] In response to these problems, law enforcement authorities have pushed for the implementation of new methods to improve the ability of law enforcement agencies to intercept criminal transmissions, while concurrently increasing the privacy of individual citizens.[3]

The "Clipper Chip" was developed to address this objective.[4] This device is intended to alleviate law enforcement's reduced ability to conduct electronic surveillance by allowing government authorities, using proper methods, to intercept criminal transmissions.[5] As planned, the Clipper Chip will achieve this by providing a mechanism for government authorities to decode encrypted communications using so-called "key escrow" technology.[6]

[1] *See* David M. Boyhan, *Cryptology to the Rescue; Codes and Cyphers Calm Security Fears*, N.Y. L.J., Nov. 9, 1993, at 5. See *infra* notes 22-28 and accompanying text for a discussion of the concerns of law enforcement and government authorities about the effects of improvements in encryption technology.

[2] John Markoff, *New Federal Electronic Privacy Policy Seen*, CHI. DAILY L. BULL., Apr. 16, 1993, at 2 [hereinafter referred to as *New Federal*].

[3] *Id.*

[4] Boyhan, *supra* note 1, at 5. In addition to other reasons, government engineers developed the Clipper Chip to prevent criminals from using advanced encryption technology to conceal their illegal activities and to provide private citizens with privacy. *Id.*

[5] *Government Issues Guidelines For Encryption Devices*, ELEC. MESSAGING NEWS, Feb. 16, 1994, at 4 [hereinafter *Government Issues*]. Law enforcement groups believe that it could more readily conduct electronic surveillance of criminals with the Clipper Chip. See *infra* notes 22-29 and accompanying text for a discussion of the reasons given by government authorities for the development of the Clipper Chip.

[6] See *infra* notes 12-21 and accompanying text for a discussion of encryption and *infra* notes 35-40 and accompanying text for a discussion of key encryption technology.

Furthermore, to implement this plan, the United States government plans to create a *de facto* standard using its purchasing power, enacting legislation which "encourages" telecommunication device vendors to include the Clipper Chip in their products and by enforcing export restrictions on encryption technology.[7]

There are conflicting reports on whether the Clinton Administration currently intends to proceed with the Clipper Chip proposal.[8] The Clinton Administration has affirmatively stated that it is considering alternatives to the Clipper Chip.[9] However, assuming the Clinton Administration decides to fully proceed with the Clipper Chip proposal, constitutional and statutory provisions exist to protect citizens from intrusions into their private communications. The Fourth Amendment protection against unreasonable searches and seizures applies to private communications which take place under a reasonable expectation of privacy. The Omnibus Crime Control and Safe Streets Act of 1968 (Title III) codifies the Supreme Court's interpretation of this provision and provides federal statutory protection for oral, wire and electronic communications by providing express requirements by which government authorities may intercept private communications for law enforcement purposes.

However, some groups believe that placing the ability to decode encrypted information in the hands of the government will enable authorities to circumvent these constitutional and federal statutory protections.[10] The fear is that the government will abuse the Clipper Chip and conduct unreasonable searches and seizures.[11] Nonetheless, these fears are unfounded if Title III ap-

[7] See *infra* notes 44-66 and accompanying text for a discussion of the government's intent to create a *de facto* encryption standard.

[8] Some reports have stated that the Clipper Chip proposal is still in limbo or on the drawing board. Penny Bender, *FBI Director May Finally Get High-Tech Snooping Devices*, GANNETT NEWS SERV., May 10, 1995, at A1. Other reports have stated the opposite and claim that the Clipper Chip proposal was abandoned in 1994. Michelle Quinn, *Decoder Policy Opposed*, S.F. CHRON., Nov. 8, 1995, at B2.

[9] John Markoff, *U.S. to Urge a New Policy on Software*, N.Y. TIMES, Aug. 18, 1995, at D1.

[10] Lance J. Hoffman, et al., *Cryptography: Policy and Technology Trends*, Dec. 1, 1993, *available in INTERNET*, Address gopher: http://www.vortex.com:/ privacy/crypt-plcy.1.z. (discussing encryption technology, market analysis of encryption technology, export controls and public policy issues). *See also* Comments of the Electronic Frontier Foundation, Testimony before the Computer System Security and Privacy Advisory Board (May 27, 1993). Such groups include the Electronic Frontier Foundation (EFF) and the Computer Professionals for Social Responsibility (CPSR). *Id.*; *see also New Federal*, *supra* note 2, at 2 (stating that "[p]eople won't be able to trust these devices because there is a high risk that the government is going to have complete access to anything they are going to do."). See *infra* notes 130-31 and accompanying text for a discussion of the concerns of these groups regarding the Clipper Chip.

[11] Edmund L. Andrews, *Federal Agencies Get Ok for High-Tech Wire Taps*, S.F.

plies to encrypted communications emanating from devices containing the Clipper Chip. Therefore, the government should not abandon the Clipper Chip proposal.

This Note examines the potential effects of the Clipper Chip if the United States Government decides to implement the Clipper Chip and the ramifications of this action for users of devices containing the chip. Part I presents the government's arguments for implementing the Clipper Chip and the manner in which the United States government intends to make it the *de facto* standard for encryption technology. Part II discusses the currently applicable constitutional analysis which applies to electronic surveillance. Part III analyzes Title III of the Federal Wiretapping Statute. Part III also examines the objections of civil libertarians to the implementation of the Clipper Chip and suggests that their fears that the device will allow the government to circumvent Constitutional and statutory protections for private communications are unfounded. Finally, Part IV discusses the current alternatives to the Clipper Chip.

I. DEVELOPMENT OF THE CLIPPER CHIP

A. Encryption

Encryption, also known as cryptography, is the art of scrambling and unscrambling voice or data transmissions.[12] Encryption allows the transmission of communications among users so that only the intended recipients are privy to the contents of a message.[13] Encryption has many common uses in society that may not be familiar to the private citizen. Among other things, encryption protects business records from unauthorized access,[14]

CHRON., Feb. 5, 1994, at A1. Privacy rights groups believe that an implemented Clipper Chip could lead to unauthorized eavesdropping because the decoder keys are in the hands of the government. *Id.* See *infra* notes 131-32 and accompanying text for a discussion of the concerns regarding increased incidence of unreasonable searches and seizures with the implementation of the Clipper Chip in telecommunications devices.

[12] Sensitive Information Could Be Regulated By Government (CNN television Broadcast, June 2, 1993). The art of encryption is as old as the alphabet. Barry D. Bayer & Benjamin H. Cohen, *E-mail and Privacy - Keeping Confidential E-mail Confidential*, LAW OFF. TECH. REV., Feb. 22, 1994, at A1. A common type of encryption is the private key. *Id.* In each communication, a private key replaces each letter in a message with a substitute. *Id.* The other party will reverse the substitution to decrypt the message. *Id.* The encrypted message will be secure as long as no one else has that key. *Id.*

[13] For example, User 1 sends the message: "Hello, my name is President Clinton." When encrypted the transmission might look something like this "xtr378 9gndki ehsdjk dsio3j38jjk8" and would sound like static in a voice transmission. However, User 2 has access to the encryption code and will be able to decode and understand its message.

[14] John Schwartz, *The Software Security 'Threat' U.S. Fears Foreign Use Of*

protects the personal information of bank customers who use automatic teller machines[15] and scrambles the video signals of cable television companies.[16] Moreover, as technology becomes more advanced, so does the sophistication and availability of encryption technology.[17] Therefore, it is logical to conclude that additional uses for encryption will arise in the future.

Today, encryption techniques, most commonly contained in computer software, scramble voice or data transmissions[18] into digital bits from the sender and unscramble the transmission for the receiver.[19] An eavesdropper attempting to intercept the message will only hear static or read nonsense unless that eavesdropper has the "key" or decoder allowing the unscrambling of digital bits. Numerous encryption technologies are in use today, but some of the more effective ones are Rivest, Shamir and Adelman (RSA)[20] and Pretty Good Privacy (PGP)[21] systems.

Encryption Features, WASH. POST, June 18, 1994, at A1 [hereinafter *Software Security*]. For example, a company can send an encrypted business plan on a disc through the mail or over a digitized line on an electronic network without the fear that a competitor could read the message in the event it was somehow intercepted. *Id.*

[15] Eric Hirschhorn & David Peyton, *Uncle Sam's Secret Decoder Ring*, WASH. POST, June 25, 1992, at A23. Many banks and other institutions rely on encryption to maintain the confidentiality of communications involving financial and other business transactions. Ivars Peterson, *Encrypting Controversy*, 143 SCI. NEWS 394, at 395.

[16] Hirschhorn & Peyton, *supra* note 15, at A23. In addition, physicians rely on encryption to protect patient files and businesses use it to keep employees records secret. *Id.*

[17] *See generally* Charles L. Evans, *U.S. Export Controls of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets*, 19 N.C. J. INT'L LAW & COM. REGUL. 469 (1994).

[18] *New Federal*, *supra* note 2, at 2. The encryption technology scrambling the transmission into digital bits may be so strong that even the National Security Agency's code breaking computers cannot unscramble the message. *Id.* Computer hardware and software can encrypt phone conversations and computer data. *Id.* Computer experts expect the number of individuals encrypting their communications will grow into wireless networks. *Id.* This will occur as a result of the nation's commerce shifting to this form of business. *Id.* Encryption is especially needed on these networks because they are particularly subject to eavesdropping. *Id.*

[19] Peterson, *supra* note 15, at 394. *See also* Evans, *supra* note 17, at 472. Encryption devices are based on the science cryptography. *Id.* Two primary encryption systems are in use today: a single key system and a two key system. *Id.* A single key system encrypts and decrypts data using the same key. *Id.* The Data Encryption Standard (DES) uses the single key. *Id.* DES has a 56 bit key length, which gives 70 quadrillion possible key combinations. *Id.* A two key system uses a pair of keys to encrypt and decrypt data. *Id.* The public-key system is a common two-key system. *Id.* In this system, a public key is available to everyone, and a secret key is known only to its owner. *Id.* The possible key combinations equal an approximately 200 digit number. *Id.*

[20] Hoffman et al., *supra* note 10, at 6. RSA is named after its inventors Rivest,

B. The Effect of Readily Available Encryption Technology

Presently, anyone can obtain encryption devices for voice or data transmissions.[22] Unfortunately, this group may include criminals, terrorists and drug dealers.[23] Law enforcement groups believe this could soon create a devastating problem because these authorities commonly rely on electronic surveillance, also known as "wiretapping," as a tool for fighting crime. That is, if criminals can use advanced encryption technology in their transmissions, electronic surveillance techniques could be rendered useless because of law enforcement's inability to decode the message.[24] As a result, computers and telecommunications systems may become safe havens for all groups of criminals, thus allowing illegal activity to increase while decreasing the ability of law enforcement to combat the crime.[25]

Furthermore, the increasing reliance of government agencies on public computer networks also presents legitimate security issues. For example, over ninety-five percent of the military's communications are routed through the same telephone network that private citizens use daily.[26] These communications include the designing of weapons, the guiding of missiles, the managing of medical supplies, the mobilization of reservists and the relaying of battle tactics to combat commanders.[27] Consequently, the military contends that maintaining the security of these transmissions is necessary and argues that the need for improved encryption techniques is vital to national security.[28] Thus, a need clearly exists to assure that this information is kept out of the "wrong hands," while assuring that the necessary authorities maintain

Shamir and Adelman and is the most popular public-key algorithm. *Id.* It is based on the theory that multiplying the private-key and public-key bits produces a prime number that is extremely difficult to break. *Id.* Devices with RSA encryption are available domestically and abroad. *Id.*

[21] *Id.* PGP is the acronym for Pretty Good Privacy. *Id.* A cryptographer named Philip Zimmerman developed this technology in response to the unavailability of free, strong, encryption technology. *Id.* PGP is a public-key system, originally based on RSA, but now combines the International Data Encryption Algorithm (IDEA) and the DES algorithm. *Id.* PGP multiplies private-key and public-key bits to produce a strong algorithm virtually uncrackable. *Id.*

[22] Boyhan, *supra* note 1, at 5.

[23] *Id.*

[24] *New Federal, supra* note 2, at 2.

[25] *Id.*

[26] Neil Munro, *The Pentagon's New Nightmare: An Electronic Pearl Harbor*, WASH. POST, July 16, 1995, at C3.

[27] *Id.* In addition, the military's communications include paying of soldiers, training tank crews, issuing press releases, controlling radio networks and finding spare parts. *Id.*

[28] *Id.*

necessary access.

C. The Clinton Administration's Response to the Problem

The concerns of law enforcement and government security have not gone unheeded; rather, the United States Government has reacted swiftly to concerns about the rapid advance of encryption technology in the private sector. In April 1993, the Clinton Administration proposed the "Clipper Chip Initiative" in an attempt to address the concerns of law enforcement and to maintain the security of confidential government communications.[29]

The Clipper Chip is a relatively inexpensive piece of hardware, costing approximately twenty-five dollars each in lots of 10,000.[30] The chip uses a classified "Skipjack algorithm"[31] which is sixteen million times more effective[32] than the currently used Data Encryption Standard (DES).[33] Each chip will have a

[29] Hoffman et al., *supra* note 10, at 6. The stated objective of the Initiative is to: "involve the creation of new products to accelerate the development and use of advanced and secure telecommunications networks and wireless communication links." *Id.* What ultimately became the Initiative actually began during the Bush Administration. Bruce Schneier, *Clipper Gives Big Brother Far Too Much Power*, COMPUTERWORLD, May 31, 1993, at 33. The proposal under the Initiative was developed jointly by the National Security Agency and the National Institute of Standards and Technology. Frederick Cooper III, *Clipper Chip: Does Proposal Violate Constitutional Rights? — Privacy vs. Security*, COMPUTER RESELLER NEWS, Mar. 28, 1994, at 79.

[30] Jube Shriver Jr., *Tapping into High-Tech Device Ok'd to Help Feds Monitor Computer — Encoded Calls*, L.A. TIMES, Apr. 17, 1993, at D1.

[31] Peterson, *supra* note 15, at 394. An algorithm is a mathematical recipe. *Id.* at 395. The Clipper Chip uses a classified algorithm called skipjack which is intended to replace the DES (Data Encryption Standard) as the national standard encryption device. *Clipper Chip and Capstone*, COMPUTER FRAUD & SEC. BULL., Sept. 1993. See *supra* notes 12-21 and accompanying text for a discussion of some encryption standards in use today.

[32] *In Brief Clipper Chip*, DOJ ALERT, June 6, 1994, at 10. Unless the National Security Agency grants someone permission, no one is allowed to test the Clipper Chip to determine its strength and security. Robert L. Hotz, *Computer Code's Security Worries Privacy Watchdogs*, L.A. TIMES, Oct.4, 1993, at A1. To test the chip, the NSA retained five cryptography experts to test the Clipper Chip's strength. *Id.* However, these experts were prohibited from discussing their conclusions except in the most general terms. *Id.* One of the experts, Dorothy Denning, has enthusiastically endorsed the Clipper Chip. *Dorothy Denning (U.S.A.)*, INTELLIGENCE NEWSL., Oct. 14, 1993, at 226.

[33] Hoffman et al., *supra* note 10, at 1. The International Business Machines Corporation (IBM) developed DES and released it to the public in 1977. *Id.* DES is based on a strong private-key encryption algorithm. *Id.* DES contains a 56-bit key as compared to the Clipper Chip's 80-bit key. *Id.* The algorithm becomes more effective as the number of bits in a key increases. *Id.* In 1993, the National Institute for Standards and Technology recertified DES as the national standard until 1998. *Id.* However, scientists contend that advanced and powerful computers may possibly break DES by attempting every possible combination of keys until the correct key is discovered. *Id.* Thus, DES may not be secure for very long. *Id.*

"master key" that can decode an encrypted message and allow the key holder to read the message.[34] Thus, when necessary, the government will be able to access information that it would otherwise not be able to read.

Cognizant of the fact that some may object to the ability of the government to access private information, the Administration has also attempted to balance the privacy concerns of citizens.[35] To ensure that government authorities will not circumvent established procedures which now exist to protect citizens against indiscriminate intrusion by authorities into private communications, the government proposes to maintain a copy of the encryption "key" and divide it into two parts.[36] When these two parts are used simultaneously, they will unlock an encrypted message and allow decoding and reading of the message.[37]

To further decrease the possibility that communications will be intercepted, the Administration plans to designate two different agencies, the Treasury Department and the Commerce Department, as trustees of the "keys."[38] Only upon the issuance of a court order will those agencies release their "keys" and allow law enforcement to successfully decrypt a message.[39] This system is

In contrast, the Clipper Chip is 24 bits longer than the DES's 56 bit key. *Id.* The interim report on the skipjack algorithm stated that it would take approximately 30-40 years to break Skipjack, but with the advances in technology, 12-18 years is more accurate. *Id.*

A comparison of the two codes:

	DES	*Skipjack*
Designer	IBM	NSA
Year Introduced	1976	1993
Formula	Public	Classified
Law Enforcement access	No	Yes
Key Chosen By	User	Government
Number of Keys	One	Two

Hotz, *supra* note 32, at A1.

[34] Peterson, *supra* note 15, at 395. This key will be made at the time the chip is produced. *Id.* It will also be deposited into two separate databases. *Id.* The Clinton administration's "key escrow" system differs from the public key system. David Post, *Encryption vs The Alligator Clip*, AM. LAW., Jan./Feb. 1995, at 111. Instead of the public knowing one of the keys, the government retains both "keys" that can unscramble encrypted files. *Id.* See *supra* notes 12-21 and accompanying text for a discussion of encryption devices.

[35] See *infra* notes 131-32 and accompanying text for a discussion of public concerns about implementation of the Clipper Chip in telecommunications devices.

[36] Peterson, *supra* note 15, at 395.

[37] *Id.*

[38] *Clipper Chip, 1994: Testimony Before the House of Representatives Committee on Science, Space & Technology, subcommittee on Technology, Environment and Aviation* (May 3, 1994) (statement of Raymond G. Kammer) (transcript available in Federal Document Clearing House Congressional Testimony).

[39] Peterson, *supra* note 15, at 395. However, many civil rights groups are fearful that the court order requirement will be bypassed in some situations or that it

now called "key escrow."[40]

The Clipper Chip would increase the ability of the government to pre-empt any threat to either law enforcement or government security because it would allow the decoding of encrypted communications without detection.[41] That is, the Clipper Chip has a 'back door' which would allow law enforcement to decode encrypted messages without the knowledge of either the sender and receiver.[42] Nonetheless, the proposed procedure to decode the messages calls for a court order prior to taking any action.[43]

D. Creation of a DeFacto Standard

Although the Clinton Administration contends that it does not intend to ban the use of all currently available encryption technology, evidence exists that the government intends to make the Clipper Chip the only legal standard.[44] That is, while the Administration claims that implementation of the Clipper Chip would be voluntary,[45] the government is attempting to create a *de facto* encryption standard through its purchasing power, enactment of legislation and export controls.

1. The Government's Coercive Purchasing Power

The federal government hopes to saturate the American tele-

is inevitable an unauthorized person will get a copy of the keys. Nina Schuyler, *Bugs in the System*, CAL. LAW., July 1994, at 47. See *infra* notes 131-32 and accompanying text for a further discussion of the concerns of some groups and *infra* notes 102-30 and accompanying text for a discussion of the constitutional requirements for government access to private communications.

[40] G. Burgess Allison, *Technology Update*, A.B.A. L. PRAC. MGMT., May/June 1994, at 14. The government now officially refers to the Clipper Chip as "key escrow." *Id.*

[41] *Software Security*, *supra* note 14, at A1.

[42] Bernard P. Zajac, Jr., *AT&T Aligns with VLSI for Cryptography Chips*, COMPUTER FRAUD & SEC. BULL., Apr. 1995, at A7. Whitfield Diffie, a respected cryptographer, describes the "key escrow" system in simplistic terms:

> [v]ery much like . . . the little keyhole in the back of the combination locks used on the lockers of school children. The children open the locks with the combinations, which is supposed to keep the other children out, but the teachers can always look in the lockers by using the key.

John Mintz & John Schwartz, *Chipping Away at Privacy?; Encryption Device Widens Debate Over Rights of U.S. to Eavesdrop*, WASH. POST, May 30, 1993, at H1 [hereinafter *Chipping Away*].

[43] Zajac, *supra* note 42, at A7. See *infra* notes 108-19 and accompanying text for a discussion of the methods for government authorities to obtain approval for interception of communications.

[44] Peterson, *supra* note 15, at 395.

[45] John Markoff, *Guarding Privacy in Cyberspace Federal Eavesdropping Plan Fraught*, STAR TRIB., Feb. 20, 1994, at A24. Michael Nelson, an administration official in charge of technology policy, stated that the government does not intend to require the use of the Clipper Chip as mandatory. *Id.*

communications and computer market with the Clipper Chip.[46] In an attempt to create a *de facto* standard in this manner, the National Institute of Standards and Technology began by strongly encouraging federal agencies to require placement of the Clipper Chip in the equipment they purchase from vendors.[47] For example, in early 1994, the government issued an order to federal agencies requiring the use of the Clipper Chip for unclassified communications including voice, fax and low-speed modem transmissions.[48] As a result, the government will require that all suppliers, as well as anyone who transacts business with these agencies, to include the Clipper Chip in their products.[49] Since redesign of products to exclude the Clipper Chip may not be cost effective, it is possible that virtually all communications devices will include the Clipper Chip, in effect creating a *de facto* encryption standard.[50] Additionally, the National Security Agency has proposed implementing the Clipper Chip outside the realm of government operations by installing it in every domestic telephone, computer modem and fax machine sold to the public.[51]

[46] John Schwartz, *Chopping Away at the Fundamental Freedom? Computer Firms, Rights Groups Clash with the White House Over Encryption vs. Law Enforcement*, WASH. POST, Mar. 2, 1993, at H1.

[47] Andrews, *supra* note 11, at A1.

[48] Zajac, *supra* note 42, at A7.

[49] *Id.*

[50] Andrews, *supra* note 11, at A1. Behind this concept lies a simple domino theory. *Id.* Eventually all governmental departments and agencies will use the Clipper Chip. It is then expected to spread to anyone who deals with the government. *Id.* There are many people and companies who communicate with the government, thus the government hopes the Clipper Chip spreads until eventually a *de facto* encryption standard exists. *Id.* Manufacturers failing to adopt the Clipper Chip would be unable to sell computer hardware and software in the lucrative federal market and could expect difficulty in obtaining export licenses. John Markoff, *Big Brother And The Computer Age*, N.Y. TIMES, May 6, 1993, at D1 [hereinafter Big Brother]. The government is attempting to establish a *de facto* encryption standard. *Id.* It will accomplish this by requiring governmental agencies to only purchase devices that incorporate the Clipper Chip. Post, *supra* note 34, at 111. *Id.*

It is possible that the Clipper Chip initiative is already underway; to date the government has purchased more than 17,000 Clipper Chips. Kevin Power, *NIST to Run Field Test of the Clipper Chip This Fall*, GOVT. COMPUTER NEWS, July 3, 1995, at 60. The government has also purchased approximately 30,000 Capstone Chips — the sister chip to the Clipper Chip. *Id.* The Clipper Chip encrypts low speed data and voice transmissions and the Capstone Chip encrypts high speed transmissions. Hotz, *supra* note 32, at A1.

[51] Jim Young, *The Information Highway to Hell; Threat Against the Right to Privacy; From the Editors; Editorial*, PULP & PAPER, June 1994, at 9. The National Institute of Science and Technology, Bell Atlantic and General Instruments Corp. have agreed to place the Clipper Chip in General Instruments' cable-television boxes. *Id.* The Clipper Chip may also be placed in SmartCards. *Id.* SmartCards are databases with health and financial information the size of a typical credit card. *Id.*

While the Administration claims otherwise, this proposal appears contrary to a voluntary implementation of the device in telecommunications equipment. In fact, in 1993 the FBI recommended mandatory use of the Clipper Chip.[52] President Clinton apparently agrees with this proposal, as Administration sources stated that President Clinton may propose legislation requiring the use of its "key escrow" encryption technology and banning the use of any other strong encryption technology that is not compatible with the Clipper Chip.[53] While such legislation is as yet not in place, Congress has already passed legislation responding to the advance of encryption technology.

2. *The Legislative Response to Advanced Encryption Technology*

In October, 1994, Congress enacted the Communications Assistance for Law Enforcement Act (commonly referred to as the "Digital Telephony Bill") to assist the FBI in wiretapping digital communications.[54] Congress enacted this legislation in recognition of the potential ineffectiveness of wiretapping due to the proliferation of advanced technology.[55] The Digital Telephony Bill requires a "telecommunications carrier"[56] to guarantee to the government that it has the capability, pursuant to a court order, to provide the government "call identifying information"[57] at a lo-

[52] *FBI Documents - Clipper Must be Mandatory*, NEWSBYTES NEWS NETWORK, Aug. 23, 1995.

[53] *Chipping Away*, *supra* note 42, at H1. Bill Frezza of Ericssa-G.E. Mobile Data Inc. said, "[t]he genie is already out of the bottle." *Id.* He was insinuating that the government will be unable to limit the spread on encryption even if there is a *de facto* standard. *Id.* Responding to this possibility, "[a]dministration sources said if the current plan doesn't enable the NSA and FBI to keep on top of the technology, then Clinton is prepared to introduce legislation to require use of its encryption technology, which is crackable by the NSA, and to ban use of the uncrackable gear." *Id.*

[54] Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 STAT. 4279 (codified at 18 U.S.C. §§ 1029, 2510, 2511, 2516, 2518, 2522, 2701, 3121, 3124; 47 U.S.C. §§ 154, 155, 157 to 159, 212 to 214, 220, 222 to 224, 226 to 229, 303b(a), 308, 309, 318, 328, 331, 356, 381 to 386, 410, 413, 533, 544, 554, 604, 605, 610, 612, 613, 701 note, 721, 731 to 734, 744, 751, 752, 1001, 1001 note, 1002 to 1011 (1994)).

[55] *See* Jaleen Nelson, Note, *Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and It's Effect on Free Flow of Information and Privacy*, 41 UCLA L. REV. 1139, 1139 n.1 (1994) (discussing the FBI proposed legislation to the second session of the 102nd Congress (the Digital Telephony Bill) and its possible constitutional ramifications).

[56] The term "telecommunications carrier" is defined as a person or entity engaged in the business of transmitting or switching wire or electronic communications. 47 U.S.C. § 1001(8).

[57] The term "call identifying information" is defined as the dialing or signaling information that identifies the origin, direction, destination, or termination of a communication by a customer of a telecommunications carrier. 47 U.S.C. § 1001(2).

cation other than the premises of the carrier.[58] For example, if a law enforcement agency possessed a court order for a wiretap, this legislation would require a company like AT&T to provide to that agency, at any remote location, the origin, destination and time of termination of the telephone call targeted. Moreover, Congress has authorized substantial funding for this legislation, which signifies that it is serious about its enactment.[59]

This legislation demonstrates Congress' desire to deal with the advance of encryption technology and the problems it may cause for law enforcement officials. However, as a result, the Clipper Chip might become an attractive option to telecommunications carriers because the companies can adopt it in their products as a ready-made method in which to comply with the Digital Telephony Bill. That is, the Clipper Chip already contains a "back door" for law enforcement since, under the key escrow system, government agencies already hold the means by which to access encrypted communications.[60] The government may hope this attractiveness will help to institute the Clipper Chip as a *de facto* encryption standard for the telecommunications industry. Export controls on encryption technology also serve as a means by which the government can push telecommunications companies toward use of the Clipper Chip.

3. Export Controls on Encryption Technology

Highly secret government communications are constantly transmitted over public computer networks.[61] Additionally, the United States government considers encryption technology in the possession of foreign countries a threat to national security.[62] Accordingly, the Department of Defense classifies encryption software as "Munitions" under the Arms Export Control Act and subjects the software to strict export controls.[63] Under this legislation, encryption technology is treated as vital to national security and a distributor must thus obtain an export license from the

[58] *Information Superhighway: An Overview Of Technology Challenges*, GENERAL ACCOUNTING OFFICE REPORT 1 (1995).

[59] *Id.* Congress apportioned $500 million to implement this program and authorized the reimbursement of reasonable costs to the telecommunications carrier. *Id.*

[60] See *supra* notes 35-40 and accompanying text for a discussion of key escrow technology.

[61] *See* Munro, *supra* note 26, at C3.

[62] Evans, *supra* note 17, at 469. The government fears that if advanced encryption technology falls into the hands of enemies of the United States the technology could become a threat to this country's national security. *Id.*

[63] *See* Arms Export Control Act § 38, 22 U.S.C. § 2778 (1988). Some other items listed on the Munitions List are: bombs, grenades, ballistic missiles, tanks, military aircraft and others. *Id.*

State Department before exporting encryption hardware or software.[64]

However, the Clinton administration has relaxed the licensing process for products exported with the Clipper Chip.[65] The apparent hope is that these relaxed standards will increase the use of the Clipper Chip by U.S. companies.[66] Any such increased usage will likely increase the success of the government's attempts to create a *de facto* standard both in the United States and possibly abroad.

The combined effect of the government's purchasing power, the enactment of the Digital Telephony Bill and export restrictions on encryption technology other than the Clipper Chip will likely effect the dynamics of a national encryption standard. The government is using these three mechanisms in an attempt to create a *de facto* encryption standard — the Clipper Chip. Implementation of this plan will certainly alleviate some concern about the use of encryption technology by criminals to circumvent discovery, as well as the concern that unauthorized people will obtain confidential government information. However, some groups fear that the government will abuse the Clipper Chip to unreasonably invade individual privacy or conduct warrantless searches and seizures. Before the concerns of these groups are addressed, a background discussion of the constitutional and statutory safeguards which protect personal communications from indiscriminate government intrusion is necessary.

II. THE FOURTH AMENDMENT AND ITS REQUIREMENTS FOR ELECTRONIC SURVEILLANCE

This Section discusses the application of the Fourth Amendment protection against unreasonable searches and seizures in the

[64] Evans, *supra* note 17, at 481-82. However, some argue that in the fast paced world of technology, U.S. exporters of software operate at a disadvantage relative to other software exporting nations because the Arms Control Export Act limits the type of encryption that may be utilized in a program, often resulting in a weaker and less desirable type being included. *Id.* at 481-82. Other countries which possess advanced encryption technology include: Germany, France, Switzerland and the United Kingdom. *Id.*

[65] *Gore Says Administration Will Work With Industry On Encryption Standard*, DAILY REP. FOR EXEC., July 22, 1994, at A19. Under current export standards, companies can export any technology using the Clipper Chip. *Id.* However, before they can export other encryption technologies, companies must continue to go through the rigors of the licensing process. *Id.*

[66] Nonetheless, the software industry is hesitant to export products with the Clipper Chip. *Chipping Away*, *supra* note 42, at H1. The Clipper Chip would be hard to sell in foreign markets because of fears that the United States Government would spy on users. *Id.* As a result, industry is hesitant to export the Clipper Chip. *Id.*

context of electronic surveillance by government authorities. This Section will address the Supreme Court decisions in *Olmstead*,[67] *Katz*[68] and *Berger*,[69] cases which laid forth the standard that electronic surveillance of wire and oral communications must satisfy under the Fourth Amendment.

The Fourth Amendment guarantees citizens security against unreasonable searches and seizures by government authorities.[70] As interpreted by the courts, the provision limits law enforcement's power to conduct a search and seizure on private citizens.[71] Thus, in order for a law enforcement officer to conduct a search or seizure, he must obtain a warrant only after making a showing of probable cause and particularly describing the purpose of the warrant.[72] Evidence obtained violating the Fourth Amendment must be excluded from trials.[73] This exclusionary rule applies to telephone surveillance.

Telephone surveillance, or "wiretapping," by government authorities began in the early part of this century. The Supreme Court first examined telephone wiretaps in *Olmstead v. United States*.[74] In this case, law enforcement agents wiretapped the defendant's telephone line away from the defendant's property.[75] The Court held that the Fourth Amendment did not apply to oral conversations over phone lines and, thus, that wiretapping by government authorities was constitutional.[76] The majority further held that the Fourth Amendment only applied to the person,

[67] Olmstead v. United States, 277 U.S. 438 (1928).

[68] Katz v. United States, 389 U.S. 347 (1967).

[69] Berger v. New York, 388 U.S. 41 (1967).

[70] U.S. CONST. amend IV. The provision reads:

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

Id.

However, the Fourth Amendment does not grant a general right to privacy. *Katz*, 389 U.S. at 350. Instead, it protects individual privacy from the government intrusion into private affairs. *Id.*

[71] *Katz*, 389 U.S. at 347; *Berger*, 388 U.S. at 41.

[72] U.S. CONST. amend IV.

[73] Weeks v. United States, 232 U.S. 383, 392 (1914). The exclusionary rule bars evidence from being admitted in a trial and is a remedy for a violation of the Fourth Amendment. *Id.*; *see also* Silverthorne Lumber Co. v. United States, 251 U.S. 385, 394 (1920) (holding that evidence obtained violating the Fourth Amendment must be excluded from trial).

[74] 277 U.S. 438 (1928).

[75] *Id.* at 457. The defendant unlawfully sold liquor violating the National Prohibition Act. *Id.* at 456. Federal officers wiretapped telephones outside the defendant's home and office. *Id.*

[76] *Id.* at 466.

home, papers and property.[77] Therefore, the Court determined that no search or seizure occurred during the telephone surveillance because law enforcement did not enter the defendants property to execute the wiretap.[78]

However, Justice Brandeis vehemently dissented stating that the Fourth Amendment should protect oral conversations to prevent law enforcement from obtaining unfettered access to private telephone conversations.[79] The Supreme Court would later adopt Justice Brandeis' reasoning in *Katz v. United States*[80] and *Berger v. New York*,[81] thus establishing the modern day process law enforcement officials must follow to conduct an electronic surveillance.

In *Katz*, the Court found that the government conducted an unreasonable search of the defendant.[82] Law enforcement officers attached an electronic wiretapping device to a public telephone booth to record the defendant's conversation.[83] The Court reasoned that the Fourth Amendment applies to people, not places, thus expressly overruling *Olmstead*.[84] Therefore, the government authorities cannot conduct a search or seizure without a warrant if a person holds a reasonable expectation of privacy in the place searched or things seized.[85] Accordingly, the Court stated that an officer conducting a search or seizure must meet three criteria:[86] 1) the officer must begin the search with probable cause;[87] 2) the officer must limit the search in scope and duration;[88] and 3) the officer must make an effort to intercept only relevant transmissions.[89] Under this standard, the Court found that the *Katz* defendant held a reasonable expectation of privacy in his telephone communication.[90]

[77] *Id.* at 463.

[78] *Id.* The Court reasoned that no search or seizure occurred because people using telephones intend to communicate with people outside of their house. *Id.* Thus, messages intercepted outside the physical boundaries of a person's house are not within the scope of the Fourth Amendment. *Id.*

[79] *Olmstead*, 277 U.S. at 475 (Brandeis, J., dissenting). Justice Brandeis stated in his famous dissent, "[t]he greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding." *Id.*

[80] 389 U.S. 347 (1967).

[81] 388 U.S. 41 (1967).

[82] *Katz*, 389 U.S. at 359.

[83] *Id.* at 348. The petitioner was convicted of transmitting wagering information in violation of a federal statute. *Id.* FBI agents recorded his illegal conversations outside a public telephone booth. *Id.*

[84] *Id.* at 351, 353.

[85] *Id.*

[86] *Id.*

[87] *Katz*, 389 U.S. at 354.

[88] *Id.*

[89] *Id.*

[90] *See id.* at 361 (Harlan, J., concurring). Katz's reasonable expectation arose

Justice Harlan's concurrence set forth a two-prong test to determine if a person holds a reasonable expectation of privacy in his communication.[91] First, the person must hold a subjective expectation of privacy.[92] Second, a person's expectation of privacy must be one that society is prepared to recognize as reasonable.[93] This test remains the standard for determining whether an individual has a reasonable expectation of privacy.[94]

In *Berger*, the Court invalidated a New York electronic surveillance statute based on the particularity clause,[95] which requires a warrant with a specific scope of allowable search.[96] The *Berger* court clarified the requirements that an electronic surveillance statute must satisfy.[97] *Berger* provides that a neutral and detached authority may grant a wiretap if the request is based on probable cause, particularly describes the places to be searched and the things to be seized, has a limited duration and requires the warrant be returned.[98]

Together, *Katz* and *Berger* establish the criteria law enforcement must follow to conduct a valid electronic surveillance.[99]

when he shut the door of the telephone booth and expected no one else to hear his conversation. *Id.*

[91] *Id.*

[92] *Katz*, 389 U.S. at 361. A person must exhibit an actual subjective expectation of privacy. *Id.* Katz had a subjective expectation of privacy. *Id.* He shut the telephone booth door and expected no on else to listen to his call. *Id.*

[93] *Id.* A person's home is an example of a place where he or she expects privacy and would be recognized as objectively reasonable. *Id.* Katz had an objective expectation of privacy. *Id.* Katz shut the telephone booth door and paid for a call. *Id.* At that point, the telephone booth was not accessible to the public. *Id.* Therefore, once Katz shut the door, he had a reasonable expectation of privacy and it is irrelevant that the booth was located in a public area. *Id.*

[94] California v. Greenwood, 486 U.S. 35, 39 (1988); California v. Ciraolo, 476 U.S. 207, 212 (1986); Dow Chem. Co. v. United States, 467 U.S. 227, 230 (1986); Oliver v. Thornton, 466 U.S. 170, 177 (1984); United States v. Knotts, 460 U.S. 276, 280 (1983).

[95] Berger v. New York, 388 U.S. 41, 59-60 (1967).

[96] The particularity clause requires that a warrant specify the purpose and extent of the search to prevent the officer from using independent discretion. Marron v. United States, 272 U.S. 192, 196 (1927); United States v. Crozier, 777 F.2d 1376, 1380 (9th Cir. 1985).

[97] *See Berger*, 388 U.S. at 59-60.

[98] *Id.* The Court found five deficiencies in the New York statute. *Id.* First, the statute did not require law enforcement to particularly describe the conversation to be overheard. *Id.* Second, the statute allowed the wiretap to stay in place for up to 60 days without a new showing of probable cause. *Id.* Third, the warrant could be renewed without probable cause if it was in the public's best interest. *Id.* Fourth, the authority for the tap did not cease to exist after the intended conversation was overheard. *Id.* And fifth, there was no return of the warrant to the court with the results of the tap and the warrant upon expiration. *Id.*

[99] *See* Mark I. Koffsky, Comment, *Choppy Waters In The Surveillance Data Stream: The Clipper Scheme And The Particularity Clause*, 9 HIGH TECH. L.J. 131, 138 (1994) (discussing a hypothetical mandatory Clipper Chip and its effect on the

Katz concentrates on whether a person has a reasonable expectation of privacy in the place searched or things seized,[100] whereas, *Berger* dictates that an electronic surveillance statute must limit the scope of each surveillance.[101]

III. THE FEDERAL GOVERNMENTS'S RESPONSE TO *KATZ* AND *BERGER*: OMNIBUS CRIME CONTROL AND SAFE STREETS ACT OF 1968 (TITLE III)

In response to *Katz* and *Berger*, Congress enacted legislation controlling oral and wire surveillance. This legislation, commonly referred to as Title III, sets forth the statutory requirements that federal authorities must follow in an electronic surveillance. This Section details this legislation, and its 1986 amendment that included electronic communications. Additionally, this Section sets forth some cases interpreting this legislation.

A. *The Requirements for a Valid Electronic Surveillance under Title III*

Title III was enacted as part of the Omnibus Crime Control and Safe Streets Act of 1968.[102] As originally enacted, Title III applied to the interception of wire and oral communications by law enforcement officers.[103] Congress subsequently amended Ti-

Particularity Clause of the Fourth Amendment).

[100] *Id.* at 138.

[101] *See* United States v. Cox, 462 F.2d 1293, 1303 n.14 (8th Cir. 1972). The court outlined the nine *Berger* requirements:

> (1) that the applicant procure "[from] a neutral and detached authority," which Katz says must be a judicial officer, an order permitting the wiretap; (2) that to procure the order, or renewal thereof, the applicant must show probable cause that an offense has been or is being committed and must state with particularity (3) the offense being investigated, (4) the place being searched (i.e., the telephone being tapped or place being bugged), and (5) the things (conversations) to be seized; (6) that the order must be executed with dispatch; (7) that it must not continue beyond the procurement of the conversation sought and thereby become "a series of intrusions, searches, and seizures pursuant to a single showing of probable cause;" (8) that it overcome the lack of notice by requiring a showing of exigent circumstances as a precondition to the order; and (9) that it require a return on the warrant.

Id. The following sections of the federal electronic surveillance statute, Title III, flow respectively from the above-enumerated criteria: (1) 18 U.S.C. § 2516; (2) § 2518(1)(f) & (2); (3) § 2518(1)(b)(i); (4) § 2518(1)(b)(iii), (4)(a) & (4)(b); (5) § 2518(1)(b)(iii) and (4)(c); (6) § 2518(6); (7) § 2518(1)(d), (4)(e) and (5); (8) § 2518(1)(c), (3)(c) & (8)(d); (9) § 2518(8)(a) & (8)(b). *Id.* See *infra* notes 102-30 and accompanying text for a discussion of Title III.

[102] 18 U.S.C. §§ 2510-2521 (1968).

[103] 18 U.S.C. § 2518(1). Wire communications denote any aural transfer made with the aid of wire, cable or other such connections. 18 U.S.C. § 2510(1). As used in the Act, "aural transfer" means a transfer containing the human voice at any point between the point of origin and reception. 18 U.S.C. § 2510(18).

tle III to include electronic communication via the Electronic Communications Privacy Act (ECPA).[104] Title III accomplishes two objectives. First, it protects an individual's privacy in oral, wire and electronic communications.[105] Second, it establishes the criteria for a valid interception by law enforcement authorities.[106] However, an overriding consideration of this is an attempt to balance the needs of law enforcement with the need to protect the privacy of the individual.[107]

Under Title III, the Attorney General or a designated enforcement officer[108] may authorize an application to a federal judge for an order allowing law enforcement to intercept an oral, wire or electronic communication.[109] Any such interception order must contain several items to be valid. A judge must first determine that based on the facts probable cause exists that an individual is committing one of the enumerated offenses in § 2516 of Title III.[110] Second, a belief must also exist based on probable cause,[111] that the surveillance will produce information about that offense.[112] Third, normal investigative procedures must have failed or were too dangerous to conduct.[113] Fourth, the Attorney General or law enforcement officer must have probable cause that the place under surveillance is connected with one of

[104] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. § 1367 (1988)). The Act defines "electronic communications" as "any transfer of signs, signals, writing, images sounds, data, or intelligence of any nature transmitted . . . by a wire, radio, electromagnetic, photoelectric or photo-optical system that affects interstate commerce. . . ." 18 U.S.C. § 2510(12).

[105] Title I of the Electronic Communications Privacy Act addresses the protections from interception of wire, oral and electronic communications. *See* S. Rep. No. 541, 99th Cong., 2d Sess. 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568 (discussing the privacy afforded to various communications in an analysis of the Electronic Communications Privacy Act).

[106] *Id.* at 27-31. The Senate Report discusses applications, orders and the implementation of orders. *Id.*

[107] Scott v. United States, 436 U.S. 128, 130 (1978). See *infra* notes 120-26 and accompanying text for a discussion of the *Scott* decision.

[108] 18 U.S.C. § 2516(1) lists the positions that may authorize an application for an intercept order. "[T]he Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General or Deputy Assistant Attorney General, or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General." *Id.*

[109] *Id.*

[110] 18 U.S.C. § 2518(3)(a).

[111] A probable cause determination for the issuance of a warrant is based on a "totality-of-the circumstances" approach. Illinois v. Gates, 462 U.S. 213, 225-39 (1983).

[112] 18 U.S.C. § 2518(3)(b).

[113] 18 U.S.C. § 2518(3)(c).

the enumerated offenses.[114] In addition, each application must identify the conversation to be intercepted,[115] the nature and location of the facility to be intercepted,[116] particularly describe the type of communication to be intercepted[117] and identify the agency and officer authorizing the surveillance[118] and the length of time for the interception.[119]

Notwithstanding the above requirements, Title III contains a safeguard provision which requires quick execution of interceptions otherwise authorized and limitation of the interception to relevant communications.[120] This safeguard, referred to as the minimization requirement, is concerned with the balancing interests between wiretapping and Fourth Amendment privacy interests.[121] The 1978 case of *Scott v. United States*[122] set the standard for this requirement.

In *Scott*, law enforcement agents wiretapped the defendant's telephone.[123] However, only forty percent of all the recorded calls related to illegal activity.[124] In finding that the authorities did not violate the minimization requirement of Title III, the Supreme Court held that the minimization safeguard must be evaluated by an objective standard.[125] Nonetheless, the Court qualified the opinion by stating that the circumstances under which the telephone is used play an important part in the deter-

[114] 18 U.S.C. § 2518(3)(d).

[115] 18 U.S.C. § 2518(4)(a).

[116] 18 U.S.C. § 2518(4)(b).

[117] 18 U.S.C. § 2518(4)(c).

[118] 18 U.S.C. § 2518(4)(d). In *United States v. Chavis*, the Supreme Court held that the identification requirement of the authorizing officer is not so critical to Title III projections to require the exclusionary rule as a remedy of wrongful identity. 416 U.S. 562, 563 (1974).

[119] 18 U.S.C. § 2518(4)(e).

[120] 18 U.S.C. § 2518(5). The minimization requirement reads:

> Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

Id.

[121] Scott v. United States, 425 U.S. 917, 917-18 (1976) (Brennan, J., dissenting from denial of *certiorari*).

[122] 436 U.S. 128, 130 (1978).

[123] *Id.* at 130. Narcotics agents obtained a warrant to intercept the communications of a telephone for a period of one month. *Id.* at 130-31. The warrant contained a requirement to restrict the interceptions to those dealing with the alleged illegal activity. *Id.* at 131-32.

[124] *Id.* at 132. As such, the defendants attempted to have the evidence suppressed for failure to meet the minimization requirement. *Id.*

[125] *Id.* at 137. However, Justice Brennan dissented alleging that to solely focus on an objective standard does not satisfactorily protect privacy interests from unlimited government surveillance. *Id.* at 147 (Brennan, J., dissenting).

mination of whether the minimization requirement is satisfied.[126]

The ECPA amended the minimization requirement of Title III. The ECPA provides that law enforcement may postpone minimization of a communication if the intercepted communication is in a foreign language or code and an expert is not reasonably available during the minimization period.[127] In such a case, minimization of the communication may be accomplished "as soon as practicable" after the interception.[128]

To date, law enforcement authorities seeking to uphold interceptions of communications in a foreign language or some type of code have used this provision.[129] With the increase in the prevalence of electronic transmissions where the communication is encrypted, this provision will very likely come into play on a more frequent basis. That is, an encrypted communication whether by telephone or by computer transmission is by definition encrypted.[130] Nonetheless, government authorities seeking to obtain these transmissions will still be required to follow the requirements of Title III to gain initial permission to intercept the communication. However, some civil libertarians believe law enforcement authorities will circumvent Title III requirements if the Clipper Chip gains widespread use.

B. *Will the Clipper Chip Allow the Government to Circumvent the Protections Afforded by Title III?*

Under the Clipper Chip key escrow system, the federal government will have the ability to decode all communications using this encryption technology.[131] Since the sole means of decoding these transmissions lies with government authorities, some believe that this control of the decoder keys may reduce the protections afforded to private communications by Title III. As such, civil libertarians believe that the government will be able to indiscriminately intercept private communications emanating from devices containing the Clipper Chip. Moreover, others fear that since all communications obtained will be encrypted, there is

[126] *Id.* at 140. For example, if law enforcement taps a public phone to monitor an individual suspected of placing bets over the phone and listens to all calls regardless of who places the calls, there will be substantial doubts as to minimization. *Id.* However, if a phone in a private residence of the head of a major drug ring is tapped, a contrary conclusion may be inferred. *Id.*

[127] 18 U.S.C. § 2518(5).

[128] *Id.*

[129] United States v. London, 66 F.3d 1227, 1236-37 (1st Cir. 1995); United States v. Gambino, 734 F. Supp. 1084, 1106 (S.D.N.Y. 1990).

[130] See *supra* notes 12-21 and accompanying text for a discussion of encryption.

[131] See *supra* notes 29-40 and accompanying text for a discussion of the Clipper Chip and the key escrow system.

no way to minimize the intercepted communications as required by Title III. This will allow law enforcement officials to access private communications which have no relation to alleged criminal activity and will thus invade the privacy of users of Clipper Chip containing devices. These fears are unfounded, however, as protections afforded will apply equally to communications emanating from devices containing the Clipper Chip. The next Section addresses these issues.

C. Title III Applies to the Clipper Chip

As discussed previously, one of Title III's objectives is to protect citizens from indiscriminate intrusions into their private communications. In recent years, the nature of communication has shifted from the traditional methods of telephones, mail and face-to-face interaction. Instead, computer technology has, in many instances, replaced these methods for both business and personal communications.[132] Nonetheless, the introduction of computers as a medium is merely an extension of these more traditional forms of communication. That is, use of computers or other forms of digital devices still operate as a mechanism to communicate with others. Congress realized as much when it enacted the ECPA to apply Title III to electronic communications.

Moreover, the installation of the Clipper Chip into a telecommunications device does not alter a user's reasonable expectation of privacy in the communication. To argue as much, one would have to also propose that the knowledge that the mere fact that the government could possibly intercept one's telephone calls by means of a wiretap also results in a relinquishment of a person's reasonable expectation of privacy. This conclusion makes no sense considering that the express purpose of Title III is to assure that law enforcement authorities do not violate a person's reasonable expectation of privacy through unauthorized interception by wiretaps or other forms of interception. Under this reasoning, a person using a device in which the Clipper Chip is installed possesses a reasonable expectation that the communication will remain private and the protections of Title III apply.[133]

The purpose of the Clipper Chip is not to intercept communications, but instead, to encrypt communications or decrypt information intercepted through judicially approved methods.[134] Moreover, the requirements of Title III also apply to communications decrypted by the Clipper Chip, as such action constitutes a

[132] S. Rep. No. 541, *supra* note 105, at 2.

[133] Scott v. United States 436 U.S. 128, 134 (1978). See *supra* notes 120-26 and accompanying text for a discussion of the *Scott* decision.

[134] *Software Security*, *supra* note 14, at A1.

means of interception as used in the Act. The statute defines the term "intercept" to mean "the aural or other acquisition of the contents of any wire, oral, or electronic communication through the use of any electronic, mechanical, or other device."[135] Decryption of electronic communications emanating from the Clipper Chip containing telecommunications devices would probably fall under this definition because the term "other device" signifies that Congress did not intend for the enumerated methods to be exclusive. Thus, courts will likely find that decryption of communications using the Clipper Chip is subject to the limitations of Title III.

D. Title III will Protect Citizens from Unreasonable Government Searches and Seizures

Since Title III applies to communications emanating from devices containing the Clipper Chip, the government must follow particular requirements to conduct a valid electronic surveillance. Thus, in order to intercept such communications, including telephone or data transmissions such as computer e-mail,[136] the government would be required to obtain a warrant based upon probable cause that the targeted individual committed a crime, that the surveillance will produce information about that offense, that normal investigative procedures have failed and that the communication under surveillance is connected with the offense.[137] Therefore, a user of a device containing the Clipper Chip will be afforded the same protections now possessed by more traditional communications devices.

Moreover, if the government does intercept a communication subject to Title III, such action would not violate the provision's minimization requirement.[138] All communications where the Clipper Chip is used will be encrypted. It follows that in most circumstances the intercepted communication will contain material unrelated to any alleged illegal activity.[139] This is no different

[135] 18 U.S.C. § 2510(4).

[136] E-mail is electronic mail sent through a computer. Anne Meredith Fulton, Comment, *Cyberspace and the Internet: Who will be the Privacy Police?*, 3 COMMLAW CONSPECTUS 63, 63 n.3 (1995).

[137] See *supra* notes 108-19 and accompanying text for a discussion of the requirements for a Title III surveillance.

[138] The minimization requirement states that law enforcement agents must minimize the recording of electronic surveillance to related matters. Scott v. United States, 436 U.S. 128, 130 (1978). See *supra* notes 120-29 and accompanying text for a discussion of the minimization requirement.

[139] Since the Clipper Chip is merely a means of scrambling and unscrambling communications, the device would not be able to differentiate between related and unrelated matters and it is possible a large ratio of unrelated matters will be acquired. *Chipping Away*, *supra* note 42, at A1.

than what normally occurs with interception of telephone communications with a wiretap and any material obtained is judged under the circumstances of the acquisition.

Unlike most intercepted telephone communications, the fact that the communication is encrypted will not permit a law enforcement agent to simultaneously minimize the communication because the message will have to be recorded in its entirety and then decoded. However, an encrypted communication is in effect in code and, as such, falls under the simultaneous minimization exception to Title III.[140] Accordingly, law enforcement may postpone minimization if the intercepted communication is in code.[141] Thus, users of devices containing the Clipper Chip will possess the same protections as those afforded to users of established communications devices.

IV. ALTERNATIVES TO THE CLIPPER CHIP

Although the Clipper Chip is a sound proposal with statutory safeguards, the Clinton Administration is succumbing to opposition of the Clipper Chip and is considering alternatives to the Clipper Chip proposal.[142] The two primary alternatives are the Commercial Key Escrow and the Flag Card systems.

The Commercial Key Escrow system is based on computer software instead of hardware like the Clipper Chip.[143] When a message is encrypted under the Commercial Key Escrow system, the designer of the encryption technology creates a private key which is deposited in a "data recover center" (a trusted, non-governmental third party) and a public key for the sender of the message.[144] If law enforcement authorities desire to obtain the contents of a message, they must obtain a warrant, record the message and then use the identification of the data recovery center contained in the message to obtain the private key to unscramble the message.[145]

Another alternative under consideration is the Flag Card system. In the Flag Card system, every national government would issue computer hardware in the form of a chip called a Flag Card with that nation's cryptographic policy.[146] Users could

[140] 18 U.S.C. § 2518(5).

[141] *Id.*

[142] John Markoff, *U.S. to Urge a New Policy on Software*, N. Y. TIMES, Aug. 18, 1995, at D1. The Clinton Administration stated that it would soon propose an alternative to the Clipper Chip. *Id.*

[143] Peter H. Lewis, *International Technology; Between a Hacker and a Hard Place*, N.Y. TIMES, Apr. 10, 1995, at D1.

[144] *Id.*

[145] *Id.*

[146] Jill Gambon, *The Business of Security — The Demise of Clipper Opens up*

scramble their messages with any encryption technologies on the Flag Card.[147] Network security servers appointed by government agencies would then police the system.[148]

Neither the Commercial Key Escrow nor Flag Card systems are superior to the Clipper Chip proposal. Neither alternative guarantees that the government could easily apprehend criminals.[149] While the government holds the decoder keys in the Clipper Chip proposal and does not in either the Commercial Key Escrow or Flag Card systems, the advantages of the alternatives are neutralized because law enforcement authorities have the same access to all three systems with a court order. Furthermore, private citizens have the same protections under Title III with all three systems whether or not the government or private companies hold the decoder keys. Therefore, the government should implement the Clipper Chip proposal to achieve its stated objectives and not abandon it because of unfounded fears.

CONCLUSION

Encryption technology has the ability to provide private citizens with the most privacy protection since the Industrial Revolution. However, it is difficult to achieve a balance between privacy and security.[150] Where the nature of encryption technology is to provide privacy protection, criminals will use encryption technology to stymie law enforcement from conducting electronic surveillance.

The Clipper Chip is only an attempt to keep up with the current pace of technology. The Clipper Chip proposal explicitly mandates safeguard procedures to prevent renegade government agencies from conducting warrantless searches and seizures. Additionally, courts will find the Clipper Chip falls under the jurisdiction of Title III. Therefore, law enforcement authorities intercepting communications using the Clipper Chip will be subjected to the procedures required in Title III and private citizens will have the protections afforded by Title III. Thus, the government is barred from admitting in court communications obtained without a warrant.

It is commonly accepted that the current system for wiretap-

Encryption Technology Market, INFORMATIONWEEK, Apr. 10, 1995, at 64.

[147] Elizabeth Corcoran, *Talk Like an Encryption: In a Coding Technology Debate that pits U.S. Against Business, 3 Firms Propose Answers*, WASH. POST, Mar. 16, 1995, at B11.

[148] Gambon, *supra* note 146, at 64.

[149] Corcoran, *supra* note 147, at B11.

[150] See *Government Issues*, *supra* note 5, at 4. The Clipper Chip Initiative strikes a balance between the legitimate needs of law enforcement and national security with the needs of business and private individuals. *Id.*

ping is not an unreasonable invasion of privacy if a warrant is obtained prior to an electronic surveillance. The Clipper Chip will not provide the government with any more power to pry into individual private lives than the current system for wiretapping provides. It is only a device to maintain the current level of wiretapping ability law enforcement agencies have at their disposal. The Clipper Chip is not Orwellian;[151] it is merely a product of the evolution of the Technological Age.

Howard S. Dakoff

[151] *See* GEORGE ORWELL, 1984 5 (1949). 1984 is a fictional book depicting the future of civilization where individuals have absolutely no privacy from the government. *Id.* This book originated the now famous quote: "Big Brother is watching you." *Id.*