The Clipper Chip: How Key Escrow Threatens to Undermine the Fourth Amendment

> As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping.[1]

INTRODUCTION

As the information age matures, the rapid development of communications technology has increased the amount of information in circulation and improved both authorized and unauthorized access to that information.[2] In response, technology has developed privacy safeguards beyond those that may be provided by law alone: encryption programs.[3] Encryption of communications is an ancient field in which messages are encoded and decoded through the use of secret keys.[4] An inherent weakness of encryption, however, is that any code can be broken.[5] In response

---

[1] Olmstead v. United States, 277 U.S. 438, 476 (1928) (Brandeis, J., dissenting).

[2] Robert W. Kastenmeier et al., *Communications Privacy: A Legislative Perspective*, 1989 WIS. L. REV. 715, 715-16 (1989) (footnote omitted).

The Internet is a global computer communications network made up of over 31,311 individual networks in 78 countries. Susan Calcari, *A Snapshot of the Internet*, INTERNET WORLD, Sept. 1994, at 54, 54. At the beginning of 1994, nearly 45 billion packets of information per month were carried over the Internet. Martin E. Hellman, *Implications of Encryption Policy on the National Information Infrastructure*, COMPUTER LAW., Feb. 1994, at 28, 28. The distribution of electronic documents is a growing business practice comparable to the spread of the fax machine. *Id.* This growth in information has led to the information super-highway, also known as the National Information Infrastructure (NII) in American policy-making. *Id.* The Internet has been characterized as either the blueprint or the chief rival of the NII. *See* Roger Taylor, *Brave New Internet*, INTERNET WORLD, Sept. 1994, at 36, 40.

[3] *See* L. Detweiler, *Cryptography for the Unwashed Masses*, CONNECT, May/June 1994, at 50, 50. Encryption is the process by which information (plaintext) is converted into code (cyphertext) through the use of auxiliary information called a key. *Id.* The encryption of static information (information that is not exchanged, such as a personal computer file) is known as private key encryption, because only one person need know the key. *Id.* The standard private key encryption system is an algorithmic program known as the Data Encryption Standard (DES). *Id.*

[4] *See* Steven Levy, *Battle of the Clipper Chip*, N.Y. TIMES, June 12, 1994, § 6 (Magazine), at 44, 47. The code used by Julius Caesar in ancient Rome was a simple alphabet mixing system. *Id.* The key to the Caesar cipher required the displacement of letters by three places in the alphabet. *Id.*

[5] *See id.* ("The problem came with protecting the key."). This axiom is true because an exchange of encrypted information requires at least two people, sender and receiver, to have access to the key. *Id.* Eventually, the number of people who must have access to the key for effective communication grows so large that the system's security is compromised. *See id.*

to this problem, computer designers created a system known as public key encryption.[6]

Public key encryption provides a virtually unbreakable defense against unwanted eavesdroppers.[7] Unfortunately, this impenetrability also substantially reduces the effectiveness of court-authorized interceptions.[8] To preserve the effectiveness of law enforcement wiretaps, the Clinton Administration adopted the Clipper chip as the government standard for data encryption.[9]

The Clipper chip, also known as key escrow encryption, allows government agencies to decode any data encrypted with the technology, including computer and telephone conversations.[10] Supporters of key escrow see it as a powerful law enforcement tool that could strip away the encoded electronic secrets of drug dealers,

---

6 *Id.* at 48. Public key encryption requires two keys to exchange encrypted information. *Id.* In this system, everybody has two keys, one public, one private. *Id.* Senders encrypt the information using the receiver's public key, which is widely available, similar to a telephone number. *Id.* Once encoded with the public key, only the receiver's private key can decode the information. *Id.*

7 *Id.* For example, encrypted transmissions, such as telephone conversations and faxes, yield only the hiss of static. *Id.* at 49.

8 *See id.* at 48-49 (hypothesizing that encryption could seriously curtail law enforcement).

9 Edmund L. Andrews, *U.S. Plans to Push Giving F.B.I. Access in Computer Codes*, N.Y. TIMES, Feb. 5, 1994, at A1. The Clipper chip was initially proposed in April, 1993. *Id.* Ostensibly, the government's purpose, as set forth by Vice President Al Gore, was "to provide better encryption to individuals and businesses while insuring that the needs of law enforcement and national security are met." *Id.* at 48. The Clipper chip is a tiny computer chip, officially named the MYK-78. Levy, *supra* note 4, at 46.

Currently, the Clipper chip is used in telephones. John Markoff, *Flaw Discovered in Federal Plan for Wiretapping*, N.Y. TIMES, June 2, 1994, at A1, D17. The Tessera card, a version of the Clipper chip to be used in personal computers, is under development. *Id.*

10 Ivars Peterson, *Prying Open the Cryptographic Door*, SCI. NEWS, Feb. 12, 1994, at 100, 100. The Clipper chip is built into communications equipment, such as telephones or modems. *Id.* Clipper encrypts "digitized speech and data according to a classified mathematical formula." *Id.* The Clipper chip operates on public-key encryption theories, but a "'back door'" is built into the system that allows authorized wiretappers to intercept and decrypt the transmission. Levy, *supra* note 4, at 50.

The National Security Agency designed the Clipper chip by relying on "a strong cryptosystem based on an algorithm called Skipjack." *Id.* Skipjack is supposedly 16 million times more powerful than the previous commercial encryption standard, DES. *Id.* Clipper uses Skipjack in conjunction with a Law Enforcement Access Field (LEAF), which is basically an electronic signpost directing an intercepting agent to the correct key for deciphering the information. *Id.* The integrated system, named Capstone, could be used with telephone conversations and computer data transfers. *Id.* Clipper is a scaled-down Capstone design, and although Clipper was designed primarily for telephone use, the technology is expandable to encompass most electronic communications systems. *Id.; see* Markoff, *supra* note 9, at D17; *see also High Marks for Encryption Algorithm*, SCI. NEWS, Aug. 28, 1993, at 143, 143 (providing a technical description of the algorithmic basis for the Clipper chip design).

terrorists, and child pornographers.[11] Many opponents see Clipper as the advent of Big Brother,[12] and as a terrifying vision of bureaucratic snoops decoding private messages, financial records, and personal information.[13] While the Clipper chip may ultimately fail to fulfill either side's visions, it has already altered wiretapping's tenuous balance between Fourth Amendment concerns and law enforcement necessities.[14]

This Comment analyzes encryption technology's impact on communications and considers how the Clipper chip controversy exposes the flaws of federal wiretapping laws, particularly the requirement that authorized wiretappers minimize the amount and type of information intercepted under the federal wiretap statute. Part I examines the judicial and statutory development of authorized electronic eavesdropping. Part II focuses on judicial treatment of minimization as a safeguard of Fourth Amendment protections. Part III describes how technological advances prompted the enactment of the Electronic Communications Pri-

---

11 *Communications and Computer Surveillance, Privacy and Security: Hearing Before the Subcomm. on Technology, Environment and Aviation of the House Comm. on Science, Space, and Technology*, 103d Cong., 2d Sess. 13 (1994) [hereinafter *House Hearing*] (statement of James Kallstrom, Special Agent in Charge, F.B.I.). Some law enforcement agents believe that criminals' and terrorists' use of encryption programs could pose "an extremely serious threat to the public safety and national security." *Id.* The Clipper chip represents an effort to maintain the ability of law enforcement agents to intercept wire and electronic communications. *Id.*

12 *See* GEORGE ORWELL, 1984 5 (Signet Classic 1992) (1949). Big Brother is the omnipotent and omnipresent personification of authoritarian government in Orwell's novel. *See id.* at 26 ("Always the eyes watching you and the voice enveloping you. Asleep or awake, working or eating, indoors or out of doors, in the bath or in bed—no escape. Nothing was your own except the few cubic centimeters inside your skull."). Many opponents of the Clipper chip use Big Brother as a metaphor for their concerns about the proposal. *See* Levy, *supra* note 4, at 46.

13 Levy, *supra* note 4, at 46 ("The Cypherpunks consider the Clipper the lever that Big Brother is using to pry into the conversations, messages and transactions of the computer age."). The firestorm of controversy sparked by the Clipper chip proposal prompted one White House technology official to characterize the issue as "the Bosnia of telecommunications." *Id.* at 51.

14 *See House Hearing*, *supra* note 11, at 1 (statement of Rep. Tim Valentine, Chairman of the Subcommittee) ("As the administration moves forward with its National Information Infrastructure initiative, the problem of accommodating the information needs of law enforcement in a way that preserves privacy rights will become more severe.").

The Fourth Amendment states:

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

U.S. CONST. amend. IV.

vacy Act of 1986. Part IV follows the development of encryption technology within the context of federal regulation, and Part V discusses the various problems presented by the Clipper chip. Part VI concludes with a reassessment of the traditional balance between the Fourth Amendment and judicially authorized electronic eavesdropping.

I. A BRIEF HISTORY OF AUTHORIZED WIRETAPPING[15]

The Supreme Court first examined law enforcement wiretaps in *Olmstead v. United States.*[16] The *Olmstead* Court reviewed the federal government's prosecution of a conspiracy to possess, import, transport, and sell intoxicating liquors in violation of the Prohibition Amendment.[17] The defendant Olmstead was the leader and general manager of the conspiracy.[18] The operation was headquartered in an office building, where the illegal business transactions were initiated and consummated over several telephone lines.[19] Federal agents tapped the lines to acquire evidence of the conspiracy, and introduced transcripts of intercepted telephone calls as evidence at trial.[20]

The Court limited its inquiry to the question of whether the government violated the Fourth Amendment in intercepting the telephone conversations of the conspirators.[21] The majority held that the interception was not an unconstitutional search and

---

15 *See generally* JAMES G. CARR, THE LAW OF ELECTRONIC SURVEILLANCE (15th Re. 1994) (providing a comprehensive history and analysis of the law and practice of electronic eavesdropping); CLIFFORD S. FISHMAN, WIRETAPPING AND EAVESDROPPING (Supp. 1994) (presenting a detailed procedural handbook of wiretapping, from investigative techniques to litigation and legal analysis).

16 277 U.S. 438, 455 (1928). For a detailed, contemporary overview of the *Olmstead* decision, see Note and Comment, 27 MICH. L. REV. 78 (1928-29).

17 *Olmstead*, 277 U.S. at 455. The National Prohibition Act outlawed the manufacture, transportation, and sale of intoxicating liquor. U.S. CONST. amend. XVIII, *repealed by* U.S. CONST. amend. XXI.

18 *Olmstead*, 277 U.S. at 456.

19 *Id.*

20 *Id.* at 456-57. The taps were accomplished by inserting wires along ordinary telephone lines, ensuring that no trespass occurred on the defendants' property. *Id.* The investigating agents tapped the office phones through the basement of the commercial office building. *Id.* at 457. The agents also tapped the home telephones of four conspirators on streets near the houses. *Id.* Transcripts of conversations were exhaustive, and overwhelming evidence of a conspiracy was obtained. *Id.*

The defendants were convicted of a conspiracy in violation of the Prohibition Amendment. *Id.* at 455. The Ninth Circuit affirmed their convictions in 1927. Olmstead v. United States, 19 F.2d 842, 848 (9th Cir. 1927), *aff'd*, 277 U.S. 438 (1928).

21 *Olmstead*, 277 U.S. at 466.

seizure as defined by the Fourth Amendment.[22] The majority grounded its holding on the premise that the Fourth Amendment applies to material objects—specifically the person, home, papers, and property—and not to oral conversations.[23] Thus, because the agents did not enter the conspirators' property, the Court determined that there had been no search and no seizure.[24]

Olmstead is notable for the vigorous dissents of Justice Holmes[25] and Justice Brandeis.[26] Justice Holmes maintained that the government should not resort to criminal actions in obtaining evidence.[27] The majority avoided this question on the technical argument that the rules of evidence did not specifically limit the admissibility of evidence obtained through criminal acts.[28] Justice Brandeis, in a clairvoyant dissent, foresaw the dangers of allowing law enforcement free rein in intercepting telephone conversations.[29] The Justice seemingly predicted the capabilities of modern computer technology and the potential for its abuse by unscrupu-

---

22 *Id.* Chief Justice Taft, writing for the majority, criticized the suggestion that evidence, even if constitutionally secured, should be excluded at the courts' discretion when obtained through unethical conduct. *Id.* at 468. The Chief Justice wrote that "[a] standard which would forbid the reception of evidence if obtained by other than nice ethical conduct by government officials would make society suffer and give criminals greater immunity than has been known heretofore." *Id.*

23 *Id.* at 464. Chief Justice Taft made the eloquent distinction that oral conversations are not "things" as required by the Fourth Amendment. *Id.* The Chief Justice concluded that there had been no search, no seizure (of "things"), and no entry into the homes or offices of the conspirators. *Id.* The majority determined that the evidence was obtained solely through "the use of the sense of hearing." *Id.*

24 *Id.* The Court decided that the Fourth Amendment could not be extended to the telephone wires "reaching to the whole world from the defendant's house or office." *Id.* at 465.

25 *See id.* at 469 (Holmes, J., dissenting).

26 *See id.* at 471 (Brandeis, J., dissenting).

27 *Id.* at 470 (Holmes, J., dissenting). The majority noted that at the time of the investigation, a Washington statute made the interception of telephone or telegraph messages a misdemeanor. *Id.* at 468 (quotation omitted). Justice Holmes proffered: "I think it a less evil that some criminals should escape than that the Government should play an ignoble part." *Id.* at 470 (Holmes, J., dissenting).

28 *See id.* at 469.

29 *See id.* at 473 (Brandeis, J., dissenting). The Justice warned that "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." *Id.* at 474 (Brandeis, J., dissenting). Since 1928, technology has expanded the capabilities of telephone wires beyond voice conversations; modern telephone exchanges can also transmit paperless digitized text, such as a fax. *See* Kastenmeier, *supra* note 2, at 718 (footnote omitted). Electronic publishing offers the ability to create, distribute, and read an entire novel without producing a single sheet of paper. Colin Haynes, *Paperless Publishing: The Future Is Now*, WRITER'S DIG., Nov. 1994, at 43, 45. Text, graphics, and even crossword puzzles can be disseminated over telephone lines through the use of a modem. *Id.*

lous users of information.[30]

Soon after the Court decided *Olmstead*, Congress followed the lead of states such as Washington and essentially banned the interception and divulgence of wire communications under § 605 of the Communications Act of 1934.[31] Nevertheless, § 605 merely limited the admissibility of such intercepted communications.[32] Electronic

---

30 *See* Kastenmeier, *supra* note 2, at 716 n. 2 (quotation and citations omitted). The storage and transmission of information without hard copies is precisely the possibility described by Justice Brandeis in his *Olmstead* dissent. *See Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting); *see also* Paul Wallich, *Wire Pirates*, SCI. AM., Mar. 1994, at 90, 90-91 (discussing the amount and variety of computer information vulnerable to criminal activity on the Internet).

31 Communications Act of 1934, ch. 652, § 605, 48 Stat. 1103, 1103-04 (current version at 47 U.S.C. § 605(a) (1988)). The 1934 version provided that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person." *Id.* The current version of this statute provides an exception for authorized law enforcement agents, preserving wiretapping as a law enforcement tool. 47 U.S.C. § 605(a) (1988).

Interestingly, § 605 was further amended as part of the Cable Communications Policy Act of 1984. Cable Communications Policy Act of 1984, Pub. L. No. 98-549, § 5, 98 Stat. 2779, 2802 [hereinafter Cable Act]. The Cable Act amended § 605 to prohibit the interception of unencrypted satellite cable programming. § 5, 98 Stat. at 2802-03 (codified at 47 U.S.C. § 605(b)-(e)). Further, in 1988, Congress added yet another section to § 605 temporarily mandating that the Federal Communications Commission investigate the need for a universal encryption standard for satellite cable programming. 47 U.S.C. § 605(f)-(g).

At the time *Olmstead* was decided, no federal statute existed that limited or prohibited wiretaps. *See Olmstead*, 277 U.S. at 468 ("In the absence of controlling legislation by Congress, those who realize the difficulties in bringing offenders to justice may well deem it wise that the exclusion of evidence should be confined to cases where rights under the Constitution would be violated by admitting it."). The *Olmstead* Court avoided the question of federal agents' liability for violating state law. *See id.* at 469 ("Whether the State of Washington may prosecute and punish federal officers violating this law and those whose messages were intercepted may sue them civilly is not before us.").

32 *See* Nardone v. United States, 302 U.S. 379, 382 (1937) [hereinafter *Nardone I*]. In *Nardone I*, the Court held that evidence obtained in violation of § 605 of the Federal Communications Act of 1934 was inadmissible in federal courts. *Id.* at 382. In *Nardone I*, the defendants were convicted of alcohol smuggling. *Id.* at 380. At trial, federal law enforcement agents testified to conversations overheard by tapping the defendants' telephone lines. *Id.* The Court considered a possible interpretation of *Olmstead* that suggested evidence procured through wiretaps was admissible at common law, regardless of state statutes to the contrary. *Id.* at 381 (citing *Olmstead*, 277 U.S. at 469). The majority rejected this theory, stating that the statutory language that "'no person . . . shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication'" should be construed literally to include federal law enforcement agents. *Id.* (quoting Communications Act of 1934, ch. 652, § 605, 48 Stat. 1103, 1103-04). The Court held that such evidence was inadmissible and remanded the case to the district court. *Id.* at 382, 385. Two years later, the Court reconsidered *Nardone v. United States*, this time addressing "whether or no[t] § 605 merely interdicts the introduction into

eavesdropping continued in the form of hidden microphones, or "bugs," and the resulting cases led to the development of a physical trespass test.[33] Between 1934 and 1967, the theory that electronic eavesdropping violated the Fourth Amendment only if accompanied by an unauthorized trespass served as a bright-line test in the federal courts.[34]

Wiretapping made a comeback during this period, but at the state level.[35] The Supreme Court finally addressed the conflict between state and federal wiretap law in *Berger v. New York*.[36] In *Berger*, the Court considered New York's eavesdropping statute, which allowed law enforcement agents to eavesdrop by electronic device and to intercept telephone and telegraph communications.[37] In *Berger*, police discovered a conspiracy to bribe the chairman of the New York State Liquor Authority after a bar owner filed a complaint.[38] During the course of their investigation, law enforcement agents placed court-authorized recording devices in the offices of

---

evidence in a federal trial of intercepted telephone conversations, leaving the prosecutor free to make every other use of the proscribed evidence." Nardone v. United States, 308 U.S. 338, 339 (1939) [hereinafter *Nardone II*]. The *Nardone II* Court refused to limit the prohibiting effect of § 605 to the exact conversations intercepted by unlawful wiretaps. *Id.* at 340. The majority held that the derivative use of wiretap evidence violated congressional intent. *Id.* The Court explained that to preclude the admissibility of direct wiretap evidence but to allow its use in investigations would be "'inconsistent with ethical standards and destructive of personal liberty.'" *Id.* (quoting *Nardone I*, 302 U.S. at 383).

33 *See* Goldman v. United States, 316 U.S. 129, 134 (1942) (holding that electronic eavesdropping through wall was not a Fourth Amendment violation because the interception was not accompanied by a physical trespass); On Lee v. United States, 343 U.S. 747, 751 (1952) (determining that because a recorded conversation between agent and suspect was not accompanied by a trespass, the Fourth Amendment was not violated); Silverman v. United States, 365 U.S. 505, 511, 512 (1961) (concluding that conversations recorded with a spike microphone inserted into a heating duct were inadmissible as a violation of the Fourth Amendment).

34 *See Silverman*, 365 U.S. at 510 (quotations omitted) (describing the development and rationale of the physical trespass test). The *Silverman* majority refused to deviate from the test "by even a fraction of an inch." *Id.* at 512.

35 *See, e.g.*, Act of Apr. 12, 1958, ch. 676, sec. 813-a, 1958 N.Y. Laws 786, 786-87 (permitting law enforcement wiretaps if accompanied by judicial authorization). By the Supreme Court's account, 27 states allowed some form of authorized interception of conversations. Berger v. New York, 388 U.S. 41, 48 (1967).

36 *Berger*, 388 U.S. at 48-49 (footnote omitted). For an illustration of the short-term effects of *Berger*, see generally Kenneth Ira Solomon, *The Short Happy Life of* Berger v. New York, 45 CHI.-KENT L. REV. 123 (1969).

37 *Berger*, 388 U.S. at 43 (citing Act of Apr. 12, 1958, ch. 676, sec. 813-a, 1958 N.Y. Laws 786, 786-87). The Court considered the statute in light of the Fourth, Fifth, Ninth, and Fourteenth Amendments. *Berger*, 388 U.S. at 43. The majority based its opinion on the Fourth and Fourteenth Amendments, declining to discuss the other amendments. *Id.* at 44.

38 *Berger*, 388 U.S. at 44.

two suspected conspirators.[39] The trial court admitted portions of recorded conversations into evidence, and Berger was consequently convicted of conspiracy to commit bribery.[40]

Noting that the law had not kept pace with eavesdropping technology, the Supreme Court held that oral conversations were protected under the Fourth Amendment and that the electronic interception of oral conversations through wiretapping or bugging was a search within the parameters of the Fourth Amendment.[41] Justice Clark, writing for the majority, emphasized that privacy is "'at the core of the Fourth Amendment'"[42] and that eavesdropping is an inherently broad invasion of privacy.[43]

The *Berger* Court further held that the New York statute was overbroad, intruding into a constitutionally protected area in violation of the Fourth Amendment.[44] Justice Clark determined that

---

[39] *Id.* at 45. The investigating officers obtained authorization for the eavesdrop order after equipping the original complainant, a bar owner, with a recording device. *Id.* at 44-45. The bar owner was able to record an incriminating conversation with a New York State Liquor Authority employee. *Id.* at 44. The employee advised the bar owner that a license required a $10,000 bribe, and that he should proceed by contacting a third party, a co-conspirator. *Id.* The investigating officers relied on this information to justify the placement of eavesdropping devices in the named co-conspirator's office. *Id.* at 45. Leads developed through this eavesdropping device resulted in the "bugging" of a second conspirator's office. *Id.* Subsequently, Berger was indicted for his role as a middleman between the principal conspirators. *Id.*

[40] People v. Berger, 219 N.E.2d 295, 295 (N.Y. 1966), *rev'd*, 388 U.S. 41 (1967). New York's highest court, the Court of Appeals, affirmed Berger's conviction. *Id.* at 295, 296.

[41] *Berger*, 388 U.S. at 49, 51. The Court based its holding in part on *Wong Sun v. United States*. *Id.* at 52 (quoting Wong Sun v. United States, 371 U.S. 471, 485 (1963) (proffering that illegally obtained verbal evidence may violate the Fourth Amendment)). Specifically, the *Wong Sun* majority noted that "the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of 'papers and effects.'" *Wong Sun*, 371 U.S. at 485 (citing Silverman v. United States, 365 U.S. 505 (1961)).

[42] *Berger*, 388 U.S. at 53 (quoting Wolf v. Colorado, 338 U.S. 25, 27 (1949)). Justice Clark noted that in *Camara v. Municipal Court*, the Court declared that "'[t]he basic purpose of [the Fourth] Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.'" *Id.* (quoting Camara v. Municipal Court, 387 U.S. 523, 528 (1967)).

[43] *Id.* at 56. Justice Douglas, in a concurring opinion, explained why electronic eavesdropping, including selective wiretaps, "is the greatest of all invasions of privacy." *Id.* at 64 (Douglas, J., concurring). Justice Douglas equated electronic surveillance with placing a police officer "everywhere and anywhere a 'bug' can be placed," including the bedroom, business, social gathering, and office. *Id.* at 64-65 (Douglas, J., concurring). This "invisible policeman" disturbed the Justice because people are incognizant of the invasion of their privacy. *Id.* at 65 (Douglas, J., concurring). The Justice characterized electronic eavesdropping as a "dragnet" that intrudes on the privacy of innocent people and intimate conversations. *Id.*

[44] *Id.* at 64. Justice Clark reasoned that such a broad statute threatened the home

the statute failed to impose certain constitutional standards for the issuance of a warrant authorizing an electronic eavesdrop.[45] The Court recognized the importance of electronic eavesdropping as a law enforcement tool.[46] The majority chose, however, to place the protections of the Fourth Amendment above the interests of law enforcement.[47]

The dissenting opinions argued that the Court's requirements imposed impossible barriers for any eavesdropping statute to overcome.[48] Justice Black's dissent suggested that an unreasonable animosity toward eavesdropping motivated the majority to levy its

---

and office, declaring that "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices." *Id.* at 63.

[45] *Id.* at 58-60. Specifically, the Court criticized the statute for failing to require: (1) particularity in describing the place to be searched and the person or property to be seized; (2) particularity in describing the offense that was or is about to be committed; (3) particularity in describing the conversations to be intercepted; (4) a single intrusion, search, or seizure, by instead allowing a two-month period of eavesdropping; (5) a prompt execution of the eavesdrop warrant; (6) a limit on the indiscriminate seizure of conversations without relevance to the offense under investigation; (7) a present probable cause for an extension of the order; (8) a termination date once the sought conversation has been obtained; (9) a showing of special circumstances to overcome defects of lack of prior notice; and (10) a return on the judicial order showing what conversations were intercepted and to what use they would be put. *Id.* The Court summarized: "[i]n short, the statute's blanket grant of permission to eavesdrop is without adequate judicial supervision or protective procedures." *Id.* at 60.

[46] *Id.* (citing PRESIDENT'S COMM'N ON LAW ENFORCEMENT AND ADMIN. OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 201 (1967) [hereinafter PRESIDENT'S COMM'N ON LAW ENFORCEMENT]). The relevant sections of the PRESIDENT'S COMM'N ON LAW ENFORCEMENT were included as an appendix to Justice White's dissent. *Id.* at 112 n. 3, 119 (White, J., dissenting). The findings contained in this report were the cornerstone of later federal wiretapping legislation. *See* S. REP. NO. 1097, 90th Cong., 2d Sess. 1 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112. Significantly, the President's Commission concluded that any wiretapping legislation must strike a "balance between law enforcement benefits from the use of electronic surveillance and the threat to privacy its use may entail." PRESIDENT'S COMM'N ON LAW ENFORCEMENT, *supra*, at 203. Further, the Commission recommended that any electronic surveillance powers granted by Congress "must be granted only with stringent limitations." *Id.*

[47] *Berger*, 388 U.S. at 62. Specifically, Justice Clark stated that "[i]n any event we cannot forgive the requirements of the Fourth Amendment in the name of law enforcement." *Id.*; *see also* Lopez v. United States, 373 U.S. 427, 441 (1963) (Warren, C.J., concurring) (recognizing the potential threat to privacy posed by advances in electronic communications).

[48] *See Berger*, 388 U.S. at 71 (Black, J., dissenting). Justice Black asserted without elaboration that the majority opinion "makes it completely impossible for the State or the Federal Government ever to have a valid eavesdropping statute." *Id.*; *see also id.* at 89-90 (Harlan, J., dissenting) (contending that the majority unnecessarily restrained legislative action regarding law enforcement eavesdropping); *id.* at 113 (White, J., dissenting) (arguing that the majority imposed impossible barriers to law enforcement eavesdropping). Justice Harlan maintained that the majority opinion used the Fourth Amendment "as a roadblock to the use . . . of law enforcement techniques necessary to keep abreast of modern-day criminal activity." *Id.* at 95 (Harlan, J., dis-

stringent requirements.[49]

Perhaps as a result of these criticisms, the U.S. Supreme Court softened its stance in *Katz v. United States*.[50] In *Katz*, a California court convicted the defendant for illegally transmitting gambling information by telephone.[51] During the course of their investigation, federal agents recorded the defendant's end of certain telephone conversations and introduced transcripts of them into evidence.[52] On appeal, the Ninth Circuit held that the use of these recordings did not violate the Fourth Amendment because they were not the result of a physical trespass.[53]

The Supreme Court observed that the Fourth Amendment governs the surreptitious recording of oral conversations as well as the seizure of tangible items.[54] Based on this premise, the Court explained that the Fourth Amendment's protections apply to people, not places.[55] Additionally, the Court stated that the physical

---

senting). The Justice asserted that the state statute at issue sufficiently restricted the unauthorized or excessive use of wiretaps. *Id.*

Justice Douglas answered the dissenters in a concurring opinion. *Id.* at 66-67 (Douglas, J., concurring). The Justice bluntly stated that "[w]ith all respect, my Brother Black misses the point of the Fourth Amendment. It does not make every search constitutional provided there is a warrant that is technically adequate." *Id.* at 67 (Douglas, J., concurring).

49 *Id.* at 71 (Black, J., dissenting) (footnote omitted). Justice Black opined that the majority opinion was rooted in "the Court's hostility to eavesdropping as 'ignoble' and 'dirty business' and in part because of fear that rapidly advancing science and technology is making eavesdropping more and more effective." *Id.* (quoting Olmstead v. United States, 277 U.S. 438, 470 (1928) (Holmes, J., dissenting)).

50 389 U.S. 347 (1967). For a discussion of the immediate impact of *Katz* on Fourth Amendment jurisprudence, see generally Note, *From Private Places to Personal Privacy: A Post-Katz Study of Fourth Amendment Protection*, 43 N.Y.U. L. REV. 968 (1968); *see also* Gregory E. Sopkin, Comment, *The Police Have Become Our Nosy Neighbors:* Florida v. Riley *and Other Supreme Court Deviations from* Katz, 62 U. COLO. L. REV. 407 (1991) (providing an analysis of recent Supreme Court treatment of the *Katz* decision).

51 *Katz*, 389 U.S. at 348 (footnote omitted).

52 *Id.*

53 Katz v. United States, 369 F.2d 130, 133, 134 (9th Cir. 1966), *rev'd*, 389 U.S. 347 (1967). F.B.I. agents recorded the defendant's side of several telephone conversations by placing microphones and recording tape on the top of two public telephone booths. *Id.* at 131. The recording devices did not penetrate the interior of the booths. *Id.* The appellate court determined that because "[t]here was no physical entrance into the area occupied" by Katz, his Fourth Amendment rights were not violated. *Id.* at 134; *see supra* notes 33-34 and accompanying text for a discussion of the physical trespass test.

54 *Katz*, 389 U.S. at 353 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

55 *Id.* at 351. The distinction arose from a dispute as to the meaning of the term "'constitutionally protected area.'" *Id.* Katz claimed that the telephone booth was such an area, while the government claimed it was not. *Id.* (footnote omitted). Both

trespass test no longer limited the application of the Fourth Amendment's protections.[56] Addressing the eavesdropping itself, the Court explained that the agents' surveillance was sufficiently circumscribed to satisfy the barriers erected in *Berger*.[57]

Congress took note of both *Berger* and *Katz* in developing Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[58] This legislation prohibits the interception and disclosure of communications[59] except by judicially-authorized law enforcement agents,[60] and provides the procedure to obtain a warrant to electronically intercept such communications.[61] Congress sought to balance the competing interests of privacy and law enforcement in order to guarantee the continued existence of a powerful investiga-

---

sides presented lists of "'protected areas.'" *Id.* at 351 n. 8. The Court had used the term "protected areas" in previous decisions. *Id.* at 351 n. 9 (citing *Silverman*, 365 U.S. at 510, 512; Lopez v. United States, 373 U.S. 427, 438-39 (1963); Berger v. New York, 388 U.S. 41, 57, 59 (1967)).

56 *Id.* at 352-53 (citations and quotations omitted). The majority observed that the physical trespass test relied on the notion that property interests controlled the government's ability to conduct searches and seizures. *Id.* at 353 (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967)). The *Katz* Court noted that in *Silverman*, the Court broadened the premise behind the Fourth Amendment and extended its protections beyond tangible objects to oral conversations overheard without any trespass. *Id.* (quoting *Silverman*, 365 U.S. at 511). The *Katz* majority reasoned that the extended protections of *Silverman* and the abandonment of "constitutionally protected areas" established that the scope of the Fourth Amendment did not "turn upon the presence or absence of a physical intrusion into any given enclosure." *Id.*

57 *Id.* at 354; *see supra* note 45 (listing the constitutional standards enumerated by the *Berger* Court). The Court explained that the surveillance was limited in scope and duration, with the specific purpose to establish the contents of the defendant's telephone conversations. *Id.* The Court also noted that the surveillance did not begin until the agents had established a strong probability that Katz was, in fact, using the telephone for illegal interstate gambling. *Id.* Finally, the Court recounted, the investigating agents confined their electronic surveillance to the times Katz used the telephone. *Id.* (footnote omitted). The Court overturned Katz's conviction, however, on the grounds that the agents acted without judicial authorization, thereby obtaining the evidence without a warrant. *Id.* at 358, 359.

58 Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified at 18 U.S.C. §§ 2510-2520 (1988)). Congress specifically drafted Title III to conform with *Katz* and *Berger*. S. REP. No. 1097, 90th Cong., 2d Sess. 28 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2113 (citing Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967)). Title III is also known as the Wiretap Act. Kastenmeier, *supra* note 2, at 717.

59 18 U.S.C. § 2511(1).

60 18 U.S.C. § 2516. Other persons excepted from Title III include officers, employees, or agents of common carriers in the ordinary course of employment, Federal Communications Commission personnel in the course of employment, parties to the conversation with prior consent, and the President of the United States in the interest of national security. 18 U.S.C. § 2511(2).

61 18 U.S.C. § 2518.

tive tool within the confines of the Fourth Amendment.[62]

Congress limited the applicability of judicially-authorized interceptions to certain enumerated offenses.[63] Title III also pro-

---

[62] S. REP. No. 1097, at 66, *reprinted in* 1968 U.S.C.C.A.N. at 2153. Congress had a dual purpose in mind for Title III: (1) to protect the privacy of both wire and oral communications, and (2) to provide a uniform basis for the authorized interception of such communications. *Id.* Congress noted that as science and technology advance, the potential to use and abuse electronic surveillance increases. *Id.* at 67, 1968 U.S.C.C.A.N. at 2154. For this reason, Congress recognized the need to protect the privacy of communications. *Id.* at 69, 1968 U.S.C.C.A.N. at 2156. At the same time, Congress articulated that "[t]he major purpose of title III is to combat organized crime." *Id.* at 70, 1968 U.S.C.C.A.N. at 2157. Congress considered wiretapping to be a particularly effective weapon against organized crime, and endeavored to carve out a law enforcement exception to the general prohibition on intercepting wire and oral communications. *Id.* at 72, 1968 U.S.C.C.A.N. at 2159.

[63] 18 U.S.C. § 2516. The interception of wire or oral communications may be authorized in the investigation of the following crimes:

> (a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), or chapter 102 (relating to riots);
>
> (b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;
>
> (c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 224 (bribery in sporting contests), section 1084 (transmission of wagering information), section 1503 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1751 (Presidential assassinations, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), or sections 2314 and 2315 (interstate transportation of stolen property);
>
> (d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;
>
> (e) any offense involving bankruptcy fraud or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;
>
> (f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title; or
>
> (g) any conspiracy to commit any of the foregoing offenses.

18 U.S.C. § 2516(1). Title III also allows individual states to authorize interception applications under state wiretap laws. 18 U.S.C. § 2516(2). State interception applications must also be in the course of investigating certain enumerated offenses, including "murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in

vides guidelines for the disclosure and use of intercepted communications,[64] as well as a general prohibition on the admissibility of communications intercepted without prior judicial authorization.[65] In detailing the procedure for obtaining authorization to intercept wire or oral communications, Congress carefully followed the constitutional blueprint provided by the Supreme Court in *Berger*.[66]

Today, law enforcement agencies consider wiretapping to be a

---

narcotic drugs, marihuana or other dangerous drugs, or other crime[s] dangerous to life, limb, or property, . . . or any conspiracy to commit any of the foregoing offenses." *Id.* The only limit on state applications is that the offense under investigation must be punishable by more than one year in prison or designated by state statute. *Id.*

64 18 U.S.C. § 2517. These guidelines permit law enforcement agents who have obtained information through a valid and authorized interception to disclose such information as necessary and proper within the performance of their official duties. 18 U.S.C. § 2517(1)-(2). The statute provides that intercepted information may be disclosed during testimony in a criminal proceeding. 18 U.S.C. § 2517(3). If a law enforcement agent intercepts communications relating to offenses aside from those specified in the wiretap order, the agent may disclose these as well. 18 U.S.C. § 2517(5). Communications that are otherwise privileged may not be disclosed. 18 U.S.C. § 2517(4).

65 18 U.S.C. § 2515.

66 *See* S. REP. No. 1097, at 75, 1968 U.S.C.C.A.N. at 2163 ("[T]he subcommittee has used the *Berger* and *Katz* decisions as a guide in drafting title III."). The congressional effort to conform to *Berger* and *Katz* was successful: the constitutionality of Title III was affirmed in a series of federal cases. *See* United States v. James, 494 F.2d 1007, 1012-13 (D.C. Cir.) (citations omitted) (rejecting the contention that Title III is unconstitutional), *cert. denied*, 419 U.S. 1020 (1974); United States v. Cox, 462 F.2d 1293, 1304 (8th Cir. 1972) (holding that specific provisions of Title III are constitutional), *cert. denied*, 417 U.S. 918 (1974); *see also* United States v. Tortorello, 480 F.2d 764, 775 (2d Cir.) (holding that, on its face, Title III does not violate the Constitution), *cert. denied*, 414 U.S. 866 (1973); United States v. Cox, 449 F.2d 679, 687 (10th Cir. 1971) (determining that Title III was a valid act of Congress), *cert. denied*, 406 U.S. 934 (1972); United States v. Focarile, 340 F. Supp. 1033, 1038 (D. Md.) (upholding the constitutionality of Title III), *aff'd sub nom.* United States v. Giordano, 469 F.2d 522 (4th Cir. 1972), *and aff'd*, 473 F.2d 906 (4th Cir. 1973), *aff'd*, 416 U.S. 505 (1974); United States v. LaGorga, 336 F. Supp. 190, 192 (W.D. Pa. 1971) (holding that the constitutionality of Title III was prima facie established); United States v. Perillo, 333 F. Supp. 914, 923 (D. Del. 1971) (stating that Title III carries a presumption of constitutionality); United States v. Leta, 332 F. Supp. 1357, 1361 (M.D. Pa. 1971) (footnote omitted) (affirming the constitutionality of Title III on its face); United States v. Scott, 331 F. Supp. 233, 240-41 (D.D.C. 1971) (holding that Title III is constitutional but granting motion to suppress evidence obtained through a wiretap), *vacated*, 504 F.2d 194 (D.C. Cir. 1974) (vacating order to suppress), *and rev'd*, 516 F.2d 751 (D.C. Cir. 1975) (reversing district court's second order to suppress), *cert. denied*, 425 U.S. 917 (1976), *conviction aff'd*, 551 F.2d 467 (D.C. Cir. 1977), *aff'd*, 436 U.S. 128 (1978); United States v. Cantor, 328 F. Supp. 561, 569 (E.D. Pa. 1971) (concluding that Title III meets constitutional requirements); United States v. Sklaroff, 323 F. Supp. 296, 306 (S.D. Fla. 1971) (holding that Title III is constitutional); United States v. Escandar, 319 F. Supp. 295, 302 (S.D. Fla. 1970) (holding that Title III does not violate constitutional provisions), *rev'd on other grounds sub nom.*, United States v. Robinson, 468 F.2d 189 (5th Cir. 1972).

vital tool in criminal investigations and prosecutions.[67] Nevertheless, wiretapping is not a common investigative tool: only 919 federal, state, and local wiretaps were authorized in 1992.[68] The effectiveness of eavesdropping in those few cases, however, is undeniable.[69] Consequently, it is in the government's interest to further relax the safeguards that prevent more aggressive eavesdropping.[70]

II. THE MINIMIZATION LIMITATION ON TITLE III INTERCEPTIONS

Minimization is a statutory safeguard requiring authorized interceptions to be swiftly executed and limited to relevant communications.[71] This safeguard directly addresses the tension between government wiretapping and Fourth Amendment privacy interests.[72] Judicial interpretation of Title III has recognized the legislative intent to preserve citizens' right to be free from

---

67 *See House Hearing, supra* note 11, at 10 (statement of James Kallstrom, Special Agent in Charge, F.B.I.). Mr. Kallstrom emphatically stated that "[w]ithout the ability to effectively execute court orders for electronic surveillance, we would be unable to protect our Nation against foreign threats, terrorism, espionage, violent crime, drug trafficking, kidnapping, and other serious crimes." *Id.*

68 *Id.* These 919 warrants, however, involved more than 100,000 people whose conversations were intercepted and recorded. Robert Lee Hotz, *Change in Technology May Curtail Wiretaps*, L.A. TIMES, Oct. 3, 1993, at A31 [hereinafter Hotz, *Change*]. Further, these wiretaps intercepted 1.7 million conversations. Robert Lee Hotz, *Demanding the Ability to Eavesdrop*, L.A. TIMES, Oct. 3, 1993, at A1, A31 [hereinafter Hotz, *Demanding*].

69 *See, e.g.*, Ames Alexander, *Tapped*, ASBURY PARK PRESS, Jan. 27, 1991, at C1. In New Jersey between 1986 and 1989, electronic surveillance resulted in 631 convictions, 63 dismissals, and zero acquittals. *Id.* Nationally, between 1982 and 1991, federal and state law enforcement agencies conducted 7,467 wiretaps that led to 19,259 convictions. John Eckhouse, *FBI Talks About Tapping Computers*, S.F. CHRON., Mar. 12, 1993, at D1, D2; *see also House Hearing, supra* note 11, at 10 (statement of James Kallstrom, Special Agent in Charge, F.B.I.) (testifying that between 1982 and 1992, wiretaps led to 22,000 convictions).

70 *See* Levy, *supra* note 4, at 49 (reporting that Louis J. Freeh, Director of the F.B.I., "told Congress that preserving the ability to intercept communications legally, in the face of these technological advances, is 'the No. 1 law enforcement, public safety and national security issue facing us today.'"). By contrast, some law enforcement experts believe that other investigative techniques can fill the gaps when electronic eavesdropping fails or is not otherwise available. *Id.*

71 *See* 18 U.S.C. § 2518(5) (1988). Specifically, the minimization requirement reads in pertinent part:

> 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.

72 *See* Scott v. United States, 425 U.S. 917, 917-18 (1976) (Brennan, J., dissenting from denial of certiorari) (quotation omitted) (contending that the minimization re-

unconstitutional searches and seizures.[73] The minimization requirement, however, provided little guidance to law enforcement officers in the application of court-ordered wiretaps.[74] Generally, intercepting agents were required to take reasonable steps to avoid intercepting conversations beyond the scope of the warrant.[75] Thus, the standard depended upon the facts and circumstances of each case, resulting in continued unpredictability regarding the admissibility of intercepted communications.[76] The Supreme Court consistently denied certiorari in cases that would allow a comprehensive treatment of the question.[77]

Finally, in 1978, the Court addressed the standard for minimi-

---

quirement "'constitutes the congressionally designed bulwark against conduct of authorized electronic surveillance'").

73 *See* Gelbard v. United States, 408 U.S. 41, 48 (1972) (footnote omitted) (reiterating that privacy was a primary concern in enacting Title III); United States v. Traficant, 558 F. Supp. 996, 1001 (N.D. Ohio 1983) (citations omitted) (explaining that legislative intent was to balance protection of privacy and law enforcement); *see also supra* note 62 (providing details of the congressional intent to balance law enforcement interests with privacy rights).

74 *See* Bynum v. United States, 423 U.S. 952, 953 (1975) (Brennan, J., dissenting from denial of certiorari) ("The urgent need for guidance from this Court clearly emerges from the record in these cases. For the record fairly bristles with apparent instances of indiscriminate and unwarranted invasions of privacy of nontargets of the surveillance."); *see also Scott*, 425 U.S. at 918 (Brennan, J., dissenting from denial of certiorari) (arguing that the Court abdicates its judicial responsibility when it denies review to cases construing the congressional mandate of minimization).

75 *See* United States v. Tortorello, 480 F.2d 764, 784 (2d Cir.) (explaining that investigating agents must demonstrate a "high regard" for privacy and must take reasonable steps to avoid unnecessary interceptions), *cert. denied*, 414 U.S. 866 (1973).

76 United States v. James, 494 F.2d 1007, 1018 (D.C. Cir. 1974) (citations omitted), *cert. denied*, 419 U.S. 1020 (1974). The standard for minimization is one of reasonableness. *Id.* Therefore, unlimited, blanket interceptions of communications may or may not violate the minimization standard, depending upon the circumstances. *Id.* (citations omitted).

77 *Scott*, 425 U.S. at 925-26 (Brennan, J., dissenting from denial of certiorari) (citations omitted). Justice Brennan expressed frustration that the Supreme Court had again refused to address the issue of Title III's minimization requirement. *Id.* at 917 (Brennan, J., dissenting from denial of certiorari). The Justice proclaimed that "the Court has consistently refused, and today persists in that refusal, to confront a case presenting the minimization question and the abuse that emanates from the seizure of 'every communication that came over the wire.'" *Id.* at 925-26 (Brennan, J., dissenting from denial of certiorari). Justice Brennan pointed out that the Court denied certiorari to a similar case. *Id.* at 923-24 (Brennan, J., dissenting from denial of certiorari) (citing Walker v. United States, 425 U.S. 917 (1976)); *see also Bynum*, 423 U.S. at 952-53 (Brennan, J., dissenting from denial of certiorari) (arguing that "[t]hese cases afford the Court a particularly appropriate vehicle for fashioning principles to guide authorizing judges in administering the 'minimization' provision—guidance which is absolutely essential if the congressional mandate to confine execution of authorized surveillances within constitutional and statutory bounds is to be carried out").

zation in *Scott v. United States*.[78] In *Scott*, government agents installed a wiretap on the telephone of a suspected narcotics dealer.[79] At trial, members of the narcotics conspiracy moved to suppress all intercepted conversations.[80] By comparing the ratio of narcotics-related telephone calls to non-narcotics-related calls, the district court determined that the investigating agents utterly failed to comply with the minimization requirement, and granted the motion to suppress.[81] The court of appeals vacated the suppression order, instructing the district court to base its determination not upon the ratio of narcotics-related calls to non-relevant calls, but rather upon the reasonableness of the investigators' attempts to minimize their interceptions.[82] On remand, the district court still suppressed the evidence, finding that although the agents were aware of the minimization requirement, they made absolutely no attempt to comply with it.[83] The court of appeals again reversed, chastising the lower court for failing to apply the proper standard.[84]

---

78 436 U.S. 128, 130 (1978) (quotation omitted). For a detailed analysis of the *Scott* decision, see Christopher J. Bellotto, Casenote, 28 CATH. U. L. REV. 143 (1979).

79 *Scott*, 436 U.S. at 131-32. The wiretap application and authorization were properly executed under Title III. *Id.* at 131. The wiretap authorization named nine individuals, all suspected of participation in a narcotics conspiracy. *Id.* The authorization specifically required the agents to minimize the interception of communications extraneous to the investigation. *Id.* at 131-32 (quotation and footnote omitted). The investigating agents intercepted virtually every telephone conversation over the period of the authorization, although only 40% of the calls were narcotics-related. *Id.* at 132. As a result of the investigation, 22 people were arrested and 14 indicted on narcotics charges. *Id.*

80 United States v. Scott, 331 F. Supp. 233, 241 (D.D.C. 1971), *vacated*, 504 F.2d 194 (D.C. Cir. 1974) (vacating order to suppress), *and rev'd*, 516 F.2d 751 (D.C. Cir. 1975) (reversing district court's second order to suppress), *cert. denied*, 425 U.S. 917 (1976), *conviction aff'd*, 551 F.2d 467 (D.C. Cir. 1977), *aff'd*, 436 U.S. 128 (1978).

81 *Id.* at 248. The district court relied on the fact that while virtually every telephone conversation was intercepted, only 40% were related to the investigation. *Id.* at 247. Further, six telephone conversations between a suspect and her mother were intercepted and transcribed despite the fact that they were completely unrelated to the conspiracy. *Id.* The district court judge found that "[t]he surveilling agents did not even attempt 'lip service compliance' with the [minimization] provision of the order and statutory mandate but rather completely disregarded it. The record is devoid of any attempt, no matter how slight, to minimize the interception of unauthorized calls." *Id.*

82 United States v. Scott, 504 F.2d 194, 198, 199 (D.C. Cir. 1974), *order on remand rev'd*, 516 F.2d 751 (D.C. Cir. 1975) (reversing district court's second order to suppress), *cert. denied*, 425 U.S. 917 (1976), *conviction aff'd*, 551 F.2d 467 (D.C. Cir. 1977), *aff'd*, 436 U.S. 128 (1978).

83 United States v. Scott, 516 F.2d 751, 752-53 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 917 (1976), *conviction aff'd*, 551 F.2d 467 (D.C. Cir. 1977), *aff'd*, 436 U.S. 128 (1978).

84 *Id.* at 753, 760. The D.C. Circuit undertook "a review of the intercepted conver-

The Supreme Court held that compliance with the minimization provision must be evaluated by an objective standard, without regard to subjective intent.[85] Furthermore, the Court interpreted the word "conducted" in the statute to mean that the agents' actions, not their intentions, should be the focus of scrutiny.[86] Justice Rehnquist then addressed the objective reasonableness of intercepting every call during the course of the wiretap, admitting the *ad hoc* nature of the inquiry.[87] The Court essentially removed the intercepting agents from the loop, disregarding the agents' intent in favor of a judicial determination of what constituted a reasonable wiretap.[88] The majority reasoned that, in hindsight, an objective examination of the interceptions demonstrated that the

---

sations rather than remanding for additional consideration by the trial court." *Id.* at 753. The court of appeals explained that while the agents' subjective intent was a factor, ultimately the decision to suppress depended upon the reasonableness of the interceptions, not on the agents' willingness to minimize. *Id.* at 756. The D.C. Circuit asserted that it was impossible to identify an example of a conversation that the agents would not have intercepted had they actually attempted to minimize. *See id.* at 757 (quotation omitted). The Supreme Court denied certiorari of the appellate court's decision to deny the motion to suppress. Scott v. United States, 425 U.S. 917 (1976). On remand, the trial court convicted Scott and the other members of the conspiracy, primarily on the basis of the intercepted telephone calls. Scott v. United States, 436 U.S. 128, 134 (1978) (citations omitted). The court of appeals affirmed the unreported district court convictions without opinion. United States v. Scott, 551 F.2d 467, 467 (1977). The Supreme Court granted certiorari. Scott v. United States, 434 U.S. 888 (1977).

85 *Scott*, 436 U.S. at 137. The Court agreed with the government's argument that "[s]ubjective intent alone . . . does not make otherwise lawful conduct illegal or unconstitutional." *Id.* at 136 (footnote omitted). The Court failed to mention that wiretapping as a law enforcement tool is merely an exception to otherwise unlawful conduct. *See id.*; *cf.* 18 U.S.C. § 2511(1) (1988) (prohibiting the interception of any oral or wire communication except as otherwise provided for by statute).

86 *Scott*, 436 U.S. at 139.

87 *Id.* The Court adopted hindsight and rationalization as the standard for determining reasonableness in minimization because "there can be no inflexible rule of law which will decide every case." *Id.* This language has served as the mantra by which federal courts have fended off potential criticism of their rationalized definition of a reasonable interception. *See, e.g.*, United States v. Garcia, 785 F.2d 214, 224 (8th Cir.) (quoting *Scott*, 436 U.S. at 139) ("The standard is one of reasonableness, and each case must be examined on its particular facts; 'there can be no inflexible rule of law which will decide every case.'"), *cert. denied*, 475 U.S. 1143 (1986).

88 *See Scott*, 436 U.S. at 145 (Brennan, J., dissenting) (asserting that the Court's reasoning "blinks reality by accepting, as a substitute for the good-faith exercise of judgment as to which calls should not be intercepted by the agent most familiar with the investigation, the *post hoc* conjectures of the Government as to how the agent would have acted"); *see* Bellotto, *supra* note 78, at 152 n. 60 (asserting that the Court's holding "substantially departs from the bulk of prior minimization law in that courts may no longer consider the surveilling officers' subjective intent, *i.e.*, bad faith, when weighing the minimization effort"). Justice Rehnquist relied on traditional search and seizure analysis in developing this objective standard. *Scott*, 436 U.S. at 137 (citations omitted). The Court failed to recognize an essential characteristic of a wiretap:

wiretap could not have been reasonably minimized by screening or categorization.[89]

In a scathing dissent, Justice Brennan accused the majority of eviscerating the minimization requirement.[90] The dissent rejected the majority's conjecture as to what minimization would have been reasonable had the agents actually attempted to minimize.[91] Further, Justice Brennan asserted that the majority effectively undercut the reasoning underlying the minimization requirement; namely, that such a requirement protects privacy interests by preventing agents from intercepting and recording every telephone conversation without limitation.[92]

---

once a conversation is intercepted and recorded, it cannot be put back where it was found. Bellotto, *supra* note 78, at 154 (footnote omitted).

89 *Scott*, 436 U.S. at 142. Circuitously, the Court determined that the court of appeals had correctly concluded that, had the investigating agents been minimizing their interceptions, it would have been reasonable to intercept every call because in hindsight it was possible to interpret each call as having some relevance to the conspiracy. *Id.* at 143. For example, Justice Rehnquist pointed to the final call between a suspect and her mother, in which the mother mentioned that an alleged co-conspirator had called to ask for a phone number. *Id.* at 142-43. The interceptions also included a number of calls to the telephone company, however, to listen to the recorded weather report. *Id.* at 141-42. Subsequent commentators have criticized the Court's contention that such calls may be relevant to a narcotics conspiracy. Bellotto, *supra* note 78, at 153 (footnote omitted).

90 *Id.* at 143 (Brennan, J., dissenting). The Justice stated:

> The Court today eviscerates this congressionally mandated protection of individual privacy, marking the third decision in which the Court has disregarded or diluted congressionally established safeguards designed to prevent Government electronic surveillance from becoming the abhorred general warrant which historically had destroyed the cherished expectation of privacy in the home.

Id. at 143-44 (Brennan, J., dissenting) (footnotes omitted).

91 *Id.* at 145 (Brennan, J., dissenting). Justice Brennan referred to the majority's *ad hoc* analysis as "*post hoc* reconstruction." *Id.* The Justice also took issue with the majority's interpretation of the word "conducted" as used in the relevant statute. *Id.* at 145-46 (Brennan, J., dissenting). In fact, Justice Brennan stated that "the Court's holding permits Government agents deliberately to flout the duty imposed upon them by Congress. In a linguistic *tour de force* the Court converts the mandatory language that the interception 'shall be conducted' to a precatory suggestion." *Id.*

92 *See id.* at 147 (Brennan, J., dissenting) (citations and quotations omitted). Justice Brennan highlighted the requirement that persons must be named in the application and authorization "'only when the law enforcement authorities have probable cause to believe that that individual is "committing the offense" for which the wiretap is sought.'" *Id.* (quoting United States v. Kahn, 415 U.S. 143, 155 (1974)). Justice Brennan maintained that in deciding *Kahn*, the Court relied on the minimization provision to prevent invasions of privacy. *Id.* (quoting *Kahn*, 415 U.S. at 154-55). The Justice contended that the *Scott* majority's "decision does not take even a sidelong glance at *United States v. Kahn*, whose reasoning it undercuts, and which may now require overruling." *Id.* For a more detailed discussion of the *Kahn* decision, see *infra* note 151.

III. LEGISLATIVE RESPONSE TO NEW COMMUNICATIONS TECHNOLOGIES

Advancements in communications technologies raised serious questions in the aftermath of *Scott*.[93] Consequently, Congress passed the Electronic Communications Privacy Act of 1986 (ECPA).[94] Justice Brandeis' prediction in *Olmstead* that technology would eventually expand the telephone's capabilities beyond mere voice transmissions was reaching fruition,[95] and the ECPA amended the Title III wiretapping statute to provide for modern computer and telecommunications technologies.[96] The amended language of Title III provides for new technologies such as computers[97] and modern telecommunications networks.[98] Next, Congress expanded the list of offenses for which court-ordered eavesdropping is authorized.[99] The ECPA added two chapters to the United States Code, the first prohibiting unauthorized access

---

93 *See* Kastenmeier, *supra* note 2, at 715-16 (footnotes omitted). Congressman Kastenmeier, the Chairman of the House Judiciary Subcommittee on Courts, Intellectual Property, and the Administration of Justice, noted that "[d]espite efforts by both Congress and the courts, legal protection against the unreasonable use of modern surveillance techniques has not kept pace with technology." *Id.* at 715 n.*, 716 (footnotes omitted). Congressman Kastenmeier echoed an earlier congressional statement, made by Senator Leahy upon introduction of the Electronic Communications Privacy Act, that "the existing law is 'hopelessly out of date.'" S. REP. No. 541, 99th Cong., 2d Sess. 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556 (quotation omitted).

94 Pub. L. No. 99-508, 100 Stat. 1848 (1986).

95 *See* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting); *supra* notes 29-30 and accompanying text (analyzing Justice Brandeis's dissent in *Olmstead*). In 1974, the Supreme Court of California recognized the threat to privacy posed by advancing technology. Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1974) (footnote omitted). The Burrows majority noted that the "[d]evelopment of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds." *Id.*

96 *See* S. REP. No. 541, at 1, *reprinted in* 1986 U.S.C.C.A.N. at 3555; *cf.* Pub. L. No. 99-508 § 101, 100 Stat. at 1848-53.

97 *See* Pub. L. No. 99-508 § 101(a)(6)(C), 100 Stat. at 1849. The ECPA also provided for other communications technologies by using the term "electronic communication." *Id.* § 101(a)(6)(12), 100 Stat. at 1848-49. For example, cellular telephone technology is included within "electronic communication," but the radio transmission between a cordless telephone and its base unit is not. *Id.*, 100 Stat. at 1849.

98 Pub. L. No. 99-508 § 101(c)(4)-(8), 100 Stat. at 1851-52.

99 Pub. L. No. 99-508 § 105, 100 Stat. at 1855-56. Examples of additional offenses for which eavesdropping may be authorized include trafficking in motor vehicles and motor vehicle parts, hostage taking, fraud connected with access devices, penalties for failure to appear, crimes related to witness relocation programs, and the destruction of aircraft and aircraft facilities. § 105(a)(1)(C), 100 Stat. at 1855. Also included is the utilization of interstate commerce in committing murder for hire, racketeering, and related violent crimes. § 105(a)(1)(D), 100 Stat. at 1855. Threatening or retaliating against federal officials, destruction of energy facilities, mail fraud, and racke-

to stored wire and electronic data,[100] the second addressing new communications monitoring devices such as pen registers.[101]

Additionally, the ECPA made two minor changes in the minimization requirement of 18 U.S.C. § 2518(5).[102] First, Congress specified when the thirty-day limit on electronic surveillance should begin to toll.[103] Second, Congress provided that minimization procedures may be postponed if the intercepted communications are in a foreign language or a code until an expert in the language or code can be found.[104] As with the original 1968 Wiretap Act, Congress drafted the ECPA to protect communications privacy, both from unauthorized interceptions of electronic communications and from unconstitutional invasions by government officials.[105]

The ECPA contains two flaws: first, by extending the list of offenses that may result in authorized interceptions, Congress has made wiretapping an accessible tool in almost any investigation.[106] Second, and perhaps more importantly, Congress integrated, rather than contradicted, judicial interpretations of Title III since

---

teering influenced and corrupt organizations (RICO violations) are also included. § 105(a)(1)(E), 100 Stat. at 1855.

100 Pub. L. No. 99-508 § 201, 100 Stat. at 1860-68 (codified at 18 U.S.C. § 2701 (1988)). The Stored Wire and Electronic Communications and Transactional Records Access chapter [hereinafter S.W.E.C.T.R.A.] essentially extends the same statutory protections to static data (e.g., computer files and electronic records) that paper files enjoy. *See* 18 U.S.C. § 2701. The S.W.E.C.T.R.A. also provides that government entities may access stored data only with a properly executed warrant. 18 U.S.C. § 2703.

101 Pub. L. No. 99-508 § 301, 100 Stat. at 1868-73 (codified at 18 U.S.C. § 3121 (1988)). Pen registers are electronic devices that record the time a call is placed on a certain telephone, as well as the number called and the duration of the connection. *See* Kastenmeier, *supra* note 2, at 730 & n.101 (providing a general discussion of pen registers).

102 Pub. L. No. 99-508 § 106(c), 100 Stat. at 1856.

103 Pub. L. No. 99-508 § 106(c)(1), 100 Stat. at 1856. The Title III Wiretap Act requires that no interception exceed 30 days. 18 U.S.C. § 2518(5). The ECPA amendment specifies that the 30-day limit begins running either when the officer begins the interception or 10 days after a court order is entered, whichever is earlier. Pub. L. No. 99-508 § 106(c)(1), 100 Stat. at 1856.

104 Pub. L. No. 99-508 § 106(c)(2), 100 Stat. at 1856.

105 *See* S. REP. No. 541, at 5, *reprinted in* 1986 U.S.C.C.A.N. at 3559 (emphasizing that "the law must advance with the technology to ensure the continued vitality of the fourth amendment"). *Id.*

106 *See* Robert Corn, *Tapping New Technologies: New Law Offers Easy Listening*, NATION, Dec. 20, 1986, at 696, 696, 697. *But see* Kastenmeier, *supra* note 2, at 736 (footnotes omitted) (arguing that the addition of new offenses did not greatly affect the possible use of wiretaps in law enforcement). Congressman Kastenmeier hypothesized that almost any investigation could allege a conspiracy or racketeering charge, thus falling within the rubric of the original 1968 Act. *Id.* (footnote omitted).

1968.[107] Thus, previous decisions such as *Scott,* which compromise certain provisions of Title III,[108] are left intact.[109] While the ECPA clearly made significant strides in protecting against the interception of electronic information,[110] true security has been left to private initiative in the form of commercial encryption.[111]

IV. THE STRATEGY OF GOVERNMENT CONTROLS ON ENCRYPTION TECHNOLOGY

Because judicially authorized eavesdropping is a vital law enforcement tool,[112] the government disfavors the dissemination of encryption.[113] In response, the federal government has adopted several policies intended to limit the dissemination of private key encryption programs.[114] The federal government classifies encryption technology as munitions, which results in strict limits on the exportation of commercial encryption products.[115] This tactic,

---

107 Kastenmeier, *supra* note 2, at 735, 736. Congressman Kastenmeier explained that the codification of case law avoids the relitigation of issues that have already been settled by the courts. *Id.* at 735. The Congressman illustrated his point by referring to the deletion of the word "'existence'" of a communication, as applied to pen registers. *Id.* at 735-36 (footnotes omitted). The Supreme Court had previously held that Title III did not protect pen register information, and the ECPA merely codified this judicial interpretation. *Id.* at 736 (footnotes omitted).

108 *See supra* notes 78-92 and accompanying text for a discussion of the *Scott* decision and its attack on the minimization provision of Title III.

109 *See* Kastenmeier, *supra* note 2, at 735, 736 (footnote omitted); *see also* United States v. Donovan, 429 U.S. 413, 439 (1977) (holding that failure to name targets of interceptions with particularity as required by Title III is not fatal to the admissibility of evidence); United States v. Kahn, 415 U.S. 143, 155 (1974) (determining that unknown parties need not be named in an interception application or authorization to be brought within the scope of the interception); United States v. Chavez, 416 U.S. 562, 574-75 (1974) (stating that failure to comply with the requirements of Title III does not necessarily render interceptions unlawful).

110 *See* Kastenmeier, *supra* note 2, at 737 (asserting that "some critics have overlooked the significant civil liberty advances contained within ECPA. The protection against governmental and private interception, surveillance and use of computer transmissions was a signal improvement in the law.").

111 *See* Levy, *supra* note 4, at 46 ("High tech has created a huge privacy gap. But miraculously, a fix has emerged: cheap, easy-to-use, virtually unbreakable encryption. Cryptography is the silver bullet by which we can hope to reclaim our privacy.").

112 *See supra* notes 67-70 and accompanying text for a discussion of the use and effectiveness of judicially authorized interceptions of communications.

113 *See* Levy, *supra* note 4, at 48 (quoting Jim Kallstrom, Special Agent in Charge, F.B.I., who described the dangers of a criminal cyberfortress that repels all law enforcement efforts to gain entry).

114 *See generally* Peter Wayner, *Should Encryption Be Regulated?*, BYTE, May 1993, at 129 (discussing a variety of government policies in response to the problems posed by cryptography).

115 22 C.F.R. §§ 120.1, 121.1 Cat. XIII (b)(1) (1993). The reasoning behind this classification is that encryption could damage United States intelligence activities

however, has a number of harmful consequences.[116] Harsh export controls such as those currently enforced could seriously damage American high-tech international trade.[117] Furthermore, these ex-

---

abroad. Carol Levin, *Exporting Technology*, PC MAG., Nov. 23, 1993, at 29, 29. While implementing the Clipper chip initiative, the Clinton Administration decided to continue strict export controls on encryption technology, specifically the commercial data encryption standard DES. *Sound and Fury Over Data Encryption*, BUS. WK., Feb. 21, 1994, at 44, 44. The government said it will relax export controls, however, on products that contain the Clipper chip. Andrews, *supra* note 9, at 48.

Administration (BXA) under the auspices of the Export Administration Act of 1979. *See* 50 U.S.C. app. §§ 2401-2420 (1988); *see also* 15 C.F.R. § 799.1(a) (1993). This Act gives the federal government the authority to require a variety of export licenses for certain goods and technology. 50 U.S.C. app. § 2403(a). Among the stated purposes of the Act are to protect the United States in matters of foreign policy and national security. 50 U.S.C. app. § 2402(7)-(10); *see also* 50 U.S.C. app. §§ 2404-2405. Because encryption technology is classified as munitions for the purposes of exportation, it is excluded from the control of the BXA. 15 C.F.R. § 770.10(a) (1993). Thus, the U.S. Department of State controls the export licenses for cryptography. 22 C.F.R. § 120.1 (a) (1993); *see generally* Charles L. Evans, Comment, *U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets*, 19 N.C. J. INT'L L. & COM. REG. 469 (1994) (providing a detailed analysis of U.S. export policy and regulations as applied to encryption technology).

If encryption technology were removed from the Munitions List, strict export controls might be severely limited by § 2403(c) of the Export Administration Act, which reads in pertinent part:

> In accordance with the provisions of this Act [sections 2401 to 2420 of this Appendix], the President shall not impose export controls for foreign policy or national security purposes on the export from the United States of goods or technology which he determines are available without restriction from sources outside the United States in sufficient quantities and comparable in quality to those produced in the United States so as to render the controls ineffective in achieving their purposes, unless the President determines that adequate evidence has been presented to him demonstrating that the absence of such controls would prove detrimental to the foreign policy or national security of the United States.

50 U.S.C. app. § 2403(c) (alteration in original). There is ample evidence that strong encryption is widely available outside the United States, despite tough export license controls. Wallich, *supra* note 30, at 101 (noting that the same cryptography software barred from export by the United States is "freely available" abroad). One encryption program, "PGP," is popular around the world. *See* Levy, *supra* note 4, at 60 (citing examples of PGP's widespread use by Burmese freedom fighters in jungle camps and by former Latvian dissidents); Ronald Bailey, *Code Blues*, REASON, May 1994, at 36, 36 (stating that PGP is obtainable around the world, including Moscow and London). For a more detailed discussion of this encryption program, see *infra* note 118. The same cryptographic algorithms currently restricted as munitions are widely accessible and are sold on street corners in Moscow. Levy, *supra* note 4, at 50. Worldwide, foreign companies offer 340 encryption products. *Id.* (quotation omitted).

116 *See, e.g.*, Levin, *supra* note 115, at 29 (asserting that "the regulation has succeeded in keeping U.S. companies out of the global marketplace").

117 *See* John Carey, *Big Brother Could Hobble High Tech*, BUS. WK., Mar. 21, 1994, at 37, 37 (reporting that export controls could cost U.S. companies six billion dollars a year in lost sales); *see also* James Aley, *Spooking Exports*, FORTUNE, Apr. 4, 1994, at 30, 30

port controls present complex enforcement problems.[118]

Another government initiative aimed at preserving law enforcement wiretapping capabilities is the Communications Assistance for Law Enforcement Act, also known as the Digital Telephony Act.[119] This Act requires communications carriers to design their systems so as to preserve law enforcement wiretapping capabilities.[120] Critics have targeted the enormous cost of such a policy; redesigning the communications infrastructure could cost

---

(citing the Business Software Alliance's estimation that U.S. companies could lose six to nine billion dollars annually to foreign competitors under current export restrictions). American companies could lose this much money because encryption is not an exclusively American product. *Id.* In fact, 120 products distributed by 21 countries use the same encryption techniques as most American products. *Id.* While the Clipper chip itself may cost only $25, redesigning applications such as cellular phones could be extraordinarily expensive, further damaging the competitiveness of American exports. *Id.* The loss in export revenue may cripple U.S. research and development, leading more consumers to buy imported encryption products. *Id.*

118 *See* Levy, *supra* note 4, at 60 (illustrating the enforcement problems presented by dissemination of encryption programs). For example, a Colorado software engineer named Philip Zimmermann created a powerful public key encryption program named PGP (for Pretty Good Privacy) and distributed it at no charge around the United States. *Id.* Eventually, the program was placed on the Internet. *Id.* Instantly, any user around the world could acquire a free copy. *See id.* The United States Customs Service considered Zimmermann's distribution of PGP an exportation of munitions. *See id.*; Bailey, *supra* note 115, at 36. Zimmermann is now the subject of a grand jury probe. Levy, *supra* note 4, at 60. Several issues are involved in the prosecution of Zimmermann. *See id.* For example, it is unclear whether placing a program on the Internet actually constitutes exportation. *Id.* Also, certain Justice Department documents suggest that government regulation of encryption programs may conflict with free speech rights under the First Amendment. *Id.*; *see also* Levin, *supra* note 115, at 29 (quoting Kate Martin, director of the American Civil Liberties Union's Center for National Security Studies) ("'We think it's a violation of the First Amendment for the government to say you can't export those products because computer software is a form of speech that's given special protection.'").

119 Pub. L. No. 103-414, 108 Stat. 4279 (1994).

120 Jaleen Nelson, *Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and Its Effect on Free Flow of Information and Privacy*, 41 UCLA L. REV. 1139, 1141 (1994) (footnotes omitted). The problem for law enforcement is twofold. John Mintz & John Schwartz, *Chipping Away at Privacy?*, WASH. POST, May 30, 1993, at H1, H4. First, the proliferation of various communications carriers and of private computer networks (e.g., CompuServe, Prodigy, America Online, etc.) requires law enforcement agencies to deal with many different companies in pursuing a wiretap. *Id.* Second, communications systems are increasingly being digitized, making it more difficult to pursue a wiretap. *Id.* Instead of intercepting voice transmissions, a digitized system produces the computer equivalent, which is a combination of zeros and ones yielding a piercing electronic squeal instead of a voice. *Id.* In order to intercept digital transmissions, which include digitized telephone calls and computerized communications such as e-mail, a "port" is required to translate the digital signals to analog, or normal language. *Id.* The Digital Telephony Act requires that companies design new digital systems with enough ports to guarantee law enforcement access to all communications lines. Pub. L. No. 103-414 § 103(a), 108 Stat. at 4280-81.

several billion dollars each year.[121] Additionally, critics debate whether such radical restructuring of the nation's communications networks is necessary to maintain a reasonable wiretapping capability.[122] Finally, accessing digital communications solves only half of law enforcement's problems.[123] Once digital communications are intercepted, law enforcement may face the problem of decoding encrypted material.[124]

Anticipating this problem, in February, 1994, the Clinton Administration announced the adoption of key escrow encryption, the Clipper chip, as a national standard.[125] The premise behind key escrow is similar to public key encryption,[126] but two federal

---

121 *House Hearing, supra* note 11, at 86 (statement of David J. Farber, Professor of Telecommunications Systems, Univ. of Pennsylvania). Estimates of the cost of redesigning the nation's communications networks start at $1.5 to $3 billion annually. *Id.* The complexity of the existing system is staggering; this complexity increases as new digitization technology develops. *Id.* Meeting the mandate of the Digital Telephony Act will require a great deal of programming, money, and time. *See id.* Congress authorized initial appropriations of $500 million per year through 1998 to finance the conversion of the nation's communications infrastructure under the Digital Telephony Act. Pub. L. No. 103-414 § 110, 108 Stat. at 4288.

122 *See* Mike Godwin, *Government Eavesdropping (Thinking Clearly About Digital Telephony)*, INTERNET WORLD, Sept. 1994, at 93, 94 [hereinafter Godwin, *Government*] (noting that the government has not "shown that technical obstacles have prevented a significant number (or in fact *any* number) of cases to be investigated and prosecuted"). Clearly, advances in communications technology impede certain aspects of law enforcement, although not necessarily crippling criminal investigation. *Id.* at 94-95.

123 *See House Hearing, supra* note 11, at 11 (statement of James Kallstrom, Special Agent in Charge, F.B.I.). Mr. Kallstrom observed that

> continuing advances in telecommunications networks and the introduction of new digitally based technologies, services and features . . . . present a twofold threat to the public safety: First, the diminished ability of telecommunications service providers to provide access to communications subject to court-ordered interception, the digital telephony issue. And secondly, the diminished ability to decipher, on a real-time basis, intercepted encrypted communications, the encryption issue.

Id.

124 *Id.* Indeed, some observers speculate that the time and money expended could be wasted if wiretaps produce nothing but "the hissy white noise of encrypted phone conversations and faxes." Levy, *supra* note 4, at 49.

125 Andrews, *supra* note 9, at A1. The Clipper chip is a voluntary encryption standard to be used by both the government and the private sector. *House Hearing, supra* note 11, at 48 (statement of Raymond G. Kammer, Deputy Director, National Institute of Standards and Technology (N.I.S.T.)). Clipper is currently intended for use in the encryption of voice telephone conversations, as well as for fax and modem communications. *Id.* For a discussion of the implications of a mandatory Escrow Encryption Standard, see generally Mark I. Koffsky, Comment, *Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and the Particularity Clause*, 9 HIGH TECH. L.J. 131 (1994).

126 *See supra* notes 6-7 and accompanying text (providing a definition and discussion of public key encryption technology). While the theoretical framework is the same, the cryptographic algorithm that forms the basis of the Clipper chip is not

agencies would hold a spare key.[127] Any electronic data encrypted using the Clipper chip would resist interception by unauthorized eavesdroppers, but with a court order, law enforcement agents would be able to access the key held in escrow and decipher any Clipper-encoded message.[128] The government anticipates that its adoption of the Clipper chip will facilitate its spread as an industry standard,[129] thus providing law enforcement with the tool necessary to maintain wiretapping as an investigative procedure.[130]

V. THE SHORTCOMINGS OF CLIPPER

A. *Workability Problems in the Marketplace*

The Clipper chip has been beset by problems, beginning with the question of whether the device actually works.[131] Because the National Security Agency (N.S.A.) developed the Clipper chip secretly, the design is currently classified information.[132] Neverthe-

---

technically a public key algorithm, but a symmetric algorithm. *House Hearing, supra* note 11, at 44 (statement of Raymond G. Kammer, Deputy Director, N.I.S.T.). Basically the only distinction between the two algorithms is that Clipper uses the same algorithm, or key, to both encode and decode, instead of using two separate algorithmic keys. *Id.*

127 *House Hearing, supra* note 11, at 44-45. The algorithmic key is split into halves, and one component is sent to each of the two agencies charged with keeping the keys in escrow: the N.I.S.T. and the Treasury Department. *Id.* Both key components held by the different agencies are required to decipher the algorithmic code. *Id.* at 45.

128 *Id.*

129 *See* Vic Sussman, *Decoding the Electronic Future*, U.S. NEWS & WORLD REP., Mar. 14, 1994, at 69, 71 ("[O]nce the Internal Revenue Service, the Pentagon and other agencies order tens of thousands of Clipper phones, it will be impossible to do government business using any other equipment."). Although adoption of the Clipper chip is a voluntary standard, the government's buying power provides a heavy incentive to all encryption consumers to implement Clipper. *Id.* After announcing the Clipper chip initiative in 1993, the F.B.I. committed to purchase 9,000 Clipper-equipped telephones from AT&T. Levy, *supra* note 4, at 50. If the government successfully converts to a Clipper chip system, any public or private entity wishing to securely communicate with the government must theoretically also use a Clipper system. *Id.* Moreover, the government's purchasing power is expected to significantly lower the cost of Clipper as compared to other commercial encryption systems. *See* Levy, *supra* note 4, at 50 (comparing pre-Clipper secure phones costing $1,195 to the $10-$30 cost of Clipper technology). *But see* Aley, *supra* note 117, at 30 (noting that the conversion to a Clipper system is costly for businesses). Finally, by continuing the export restrictions on encryption technology, "the government is trying to make it difficult for any alternative schemes to become widespread." Philip Elmer-Dewitt, *Who Should Keep the Keys?*, TIME, Mar. 14, 1994, at 90, 91.

130 Levy, *supra* note 4, at 46. Levy asserted that "[b]y adding Clipper chips to telephones, we could have a system that assures communications will be private—from everybody but the Government." *Id.*

131 Markoff, *supra* note 9, at A1.

132 Sharon Begley with Melinda Liu, *Foiling the Clipper Chip*, NEWSWEEK, June 13, 1994, at 60, 62. Much of the criticism of the Clipper chip stems from the fact that the

less, several companies claim to have a patent on the underlying technology.[133] The Clipper chip has also been criticized by Matthew Blaze, an AT&T Bell Laboratories scientist, who claims that the chip may not even work.[134] According to Blaze, the escrow key may not always be able to decode data encrypted with the Clipper chip.[135] If Blaze is correct, the Clipper chip may be completely ineffective and unable to satisfy the needs of law enforcement.[136] Another possible method of circumventing the Clipper chip's back door is to simply double-encrypt by sending pre-encrypted material through a Clipper system.[137] Ultimately, the Clipper chip may be out of date before it is implemented.[138]

---

underlying technology is classified. *See House Hearing, supra* note 11, at 56 (statement of Jerry Berman, Executive Director, Electronic Frontier Foundation). As one commentator emphasized, "[t]he algorithm to Clipper is secret, so it cannot be tested. So the vast majority of the people who put the 'Good Housekeeping Seal of Approval' on this technology, say you can't trust it." *Id.*

133 Aaron Zitner, *US Wiretap Plan Runs Into Static*, BOSTON GLOBE, June 3, 1994, at 73, 75. Silvio Micali, a computer science professor at the Massachusetts Institute of Technology, claims he holds two patents covering the use of mathematical keys to decipher messages. *Id.* RSA Data Security Inc. contends that Clipper infringes on certain patents it holds. *Id.* If the Clipper chip does indeed violate these patents, then the price of the technology would undoubtedly rise as a consequence of licensing fees. *See id.* (noting that "[t]echnology royalties commonly run as high as 5 percent of the value of a product").

134 Begley, *supra* note 132, at 60.

135 *Id.* While encrypted information may be indecipherable to casual eavesdroppers, law enforcement agents also may not be able to decipher certain intercepted transmissions. *Id.* Blaze found a flaw in the way the Law Enforcement Access Field (LEAF) is transmitted at the beginning of each message. *Id.; see supra* note 10 (explaining the concept and importance of LEAF). Blaze explained that users can transmit a rogue LEAF that would provide eavesdroppers with the incorrect key. Begley, *supra* note 132, at 60. When the wrong key is used in decoding the message, agents would be unable to decipher the resulting "gibberish." *Id.* The National Security Agency acknowledged this flaw, but maintained that it does not affect Clipper's performance in voice, fax, or low-speed electronic data transmissions. *Id.* Nevertheless, Clipper may not allow law enforcement agencies to intercept and decipher computer e-mail or other high-speed data transmissions. *Id.* at 60, 62. Without that capability, Clipper is fundamentally limited in its application. *Id.* at 60.

136 Begley, *supra* note 132, at 60. Because the underlying algorithm is secret, independent testing of the Clipper chip is nearly impossible. Levy, *supra* note 4, at 70.

137 *House Hearing, supra* note 11, at 56 (statement of Jerry Berman, Executive Director, Electronic Frontier Foundation). Nothing in the Clipper chip system prevents the simultaneous use of a second encryption program to encrypt over the Clipper chip. *Id.*

138 *See* Levy, *supra* note 4, at 70. The Clipper chip was designed for use in current communications equipment. *Id.* As technology advances, however, transmission speeds will increase and Clipper will require updates. *Id.* Anticipating this problem, the National Security Agency has already developed a high speed version of the core algorithm Skipjack that surpasses the Clipper chip. *Id.* Also under development is a new key escrow encryption device known as Baton. *Id.*

The Clipper chip has also been criticized as a poor business decision.[139] While the government's buying power may make Clipper the primary domestic encryption device, many observers warn that it will never sell overseas because no foreign business or government wants a system that provides a back door to the United States government.[140] Critics also claim that by crippling domestic software designers through strict export license controls, the United States may not be competitive in the global data encryption market.[141] Moreover, criminals, knowing that their encrypted telephone calls and computer files may be deciphered by the government, will simply rely on readily available strong encryption programs instead of the Clipper chip.[142]

The fatal flaw of key escrow, however, may be best illustrated by the reasons behind the development of public key encryption.[143] Computer programmers developed public key encryption to eliminate the security gap created by dissemination of the key to third parties.[144] While the government promises stringent security in maintaining the keys in escrow,[145] observers note that trusting

---

139 *See, e.g.*, Sussman, *supra* note 129, at 69 (quoting Senator Patrick Leahy's contention that "Clipper is a 'misstep in export policy'").

140 *See* Levy, *supra* note 4, at 70 (noting that "most American telecommunications and computer manufacturers [agree] that Clipper and subsequent escrow schemes will find no favor in the vast international marketplace, turning the United States into a cryptographic island and crippling important industries").

141 Aley, *supra* note 117, at 30.

142 *See House Hearing*, *supra* note 11, at 56 (statement of Jerry Berman, Executive Director, Electronic Frontier Foundation). Mr. Berman noted that the Clipper chip

> may solve the law enforcement problem, but it only solves it if criminals use it . . . . The terrorists, the World Trade Center bombing, the international terrorist organizations—why are they going to go to Radio Shack or to wherever they buy equipment in a foreign country and buy the "Clipper Chip" which says "Made by NSA," keys held by the United States Government?

Id. Law enforcement officials have acknowledged that the Clipper chip will not be a significant aid in apprehending "smart criminals." Mike Godwin, *Privacy From Whom?*, PLAYBOY, Sept. 1994, at 41, 41 [hereinafter, Godwin, *Privacy*]. Moreover, supporters of the Clipper chip have been unable to produce evidence that encryption has ever interfered with a criminal investigation. *Id.*

143 *See* Levy, *supra* note 4, at 47 (describing the security concerns that motivated the development of public encryption); *see also supra* notes 3-7 and accompanying text (discussing the development of public key encryption). Whitfield Diffie and Martin Hellman, computer scientists at Stanford University, developed the technological breakthrough in the 1970s that led to current public key encryption systems. Levy, *supra* note 4, at 48.

144 Levy, *supra* note 4, at 48. In fact, "'[t]he virtue of cryptography should be that you don't have to trust anybody not directly involved with your communication.'" *Id.* (quoting Whitfield Diffie).

145 *See id.* at 60 (noting that the government uses four couriers to transport multiple copies of the escrow key code splits between Mykotronx, the company that manufac-

the government is not always a wise choice.[146] The Clipper chip undermines the proposition that an individual can totally control his or her privacy by managing the only key to his or her own code.[147]

B. *Legal Implications of the Clipper Chip*

Often, the legal implications of key escrow encryption are lost amid the contentious debate surrounding the Clipper chip. Despite the rhetoric of some anti-Clipper commentators, the Clipper chip does not represent a *carte blanche* for the government to spy on private citizens.[148] An important yet often underemphasized limit on law enforcement's use of key escrow is the warrant requirement.[149] The mere existence of such a requirement limits the use of key escrow to legitimate law enforcement investigations.[150] The Supreme Court has undercut the warrant requirement, however, rendering it an inadequate protection of Fourth Amendment privacy rights.[151] Where a warrant requirement falls short, the Court

---

tures the Clipper chip, and the escrow agencies, where the disks holding the codes are stored in safes).

146 Wayner, *supra* note 114, at 132-33 (quoting Bill Spernow, of Search, a non-profit corporation funded by the Justice Department that helps law enforcement agencies combat computer crime) ("'The government . . . has not historically shown the ability to keep secrets of this magnitude.'"); *see also* Sussman, *supra* note 129, at 71 (noting past abuses of the public trust by the N.S.A., F.B.I., and C.I.A.); *cf.* Godwin, *Privacy*, *supra* note 142, at 41 (asserting that entrusting the privacy of communications to the government's good faith is contrary to principles of individual liberty).

The government has also demonstrated an inability to maintain the privacy of computerized information databases, which often contain confidential information such as credit reports. *See* Jeffrey Rothfeder, *What Happened to Privacy?*, N.Y. TIMES, Apr. 13, 1993, at A21. Federal privacy laws often provide exemptions that allow an alarming number of people and organizations access to personal information stored in computerized databases. *Id.*

147 *See* Levy, *supra* note 4, at 48 (quoting Whitfield Diffie) ("'The virtue of cryptography should be that you don't have to trust anybody not directly involved with your communication.'").

148 *See* Michael Meyer & Daniel Glick, *Keeping the Cybercops Out of Cyberspace*, NEWSWEEK, Mar. 14, 1994, at 38, 38 ("The concern [about government eavesdropping] is understandable but overblown.").

149 Andrews, *supra* note 9, at 48.

150 *Cf.* Kastenmeier, *supra* note 2, at 736 (footnote omitted) (contending that almost any investigation can allege charges that would justify a wiretap).

151 *See* United States v. Kahn, 415 U.S. 143, 163 (1974) (Douglas, J., dissenting) (maintaining that under the majority's decision, "a wiretap warrant apparently need specify but one name and a national dragnet becomes operative"). *Kahn* addressed the question of who must be named in an order authorizing a wiretap interception. *Id.* at 150. In *Kahn*, a court order authorized the interception of "'wire communications of Irving Kahn and others as yet unknown.'" *Id.* at 147. Kahn's wife made two phone calls implicating her in the interstate gambling conspiracy under investigation. *Id.* The Court examined whether the intercepted communications implicating Mrs.

relies on minimization as the penultimate safeguard of privacy.[152] Ostensibly, then, the government and the courts would rely on existing safeguards under Title III to prevent the abuses that many critics predict will accompany the Clipper chip. Unfortunately, the Court has severely weakened these statutory safeguards.[153]

Kahn were admissible under the "'others as yet unknown'" language of the wiretap authorization. *Id.* at 150.

The Court held that the failure of the order to specify Mrs. Kahn did not preclude the admission of her intercepted conversations into evidence. *Id.* at 158. The Court also held that the language of the order did not require that Mr. Kahn be a party to every intercepted communication. *Id.* The Court relied in part on the language and legislative history of Title III. *Id.* at 151. The majority determined that "Title III requires the naming of a person in the application or interception order only when the law enforcement authorities have probable cause to believe that that individual is 'committing the offense' for which the wiretap is sought." *Id.* at 155. Because the government did not suspect that Mrs. Kahn was involved in the conspiracy, the Court reasoned, she was "among the class of persons 'as yet unknown' covered" by the wiretap authorization. *Id.* The Court elaborated that "Congress could not have intended that the authority to intercept must be limited to those conversations *between* a party named in the order and others, since at least in some cases, the order might not name any specific party at all." *Id.* at 157 (footnote omitted).

A similar case, *United States v. Donovan*, concerned a wiretap interception application and order that failed to name three individuals even though the government knew their identities. United States v. Donovan, 429 U.S. 413, 419 n.5 (1977). The Court determined that the government was indeed required to name with particularity the targets of the interception where the targets were known and identifiable, in accordance with the minimization statute. *Id.* at 432 (citation omitted). The Court also held that when the government supplied the supervising judge with a list of identifiable persons whose communications were intercepted, this list must be complete. *Id.* Despite the failure of the government to comply with these statutory requirements, the Court held that Title III did not require suppression of the evidence gathered in violation of the statute. *Id.* at 439-40.

Justice Brennan viewed the *Kahn* and *Donovan* decisions as major blows to "congressionally established safeguards designed to prevent Government electronic surveillance from becoming the abhorred general warrant which historically had destroyed the cherished expectation of privacy in the home." Scott v. United States, 436 U.S. 128, 143-44 (1978) (Brennan, J., dissenting) (footnotes omitted).

152 *See Scott*, 436 U.S. at 147 (Brennan, J., dissenting) (noting that the Court has "relied on the minimization requirement as an adequate safeguard to prevent . . . unlimited invasions of personal privacy"). In criticizing the *Scott* majority for weakening the minimization requirement, Justice Brennan contended that the decision undermined the Court's reasoning in *Kahn* that minimization balances any dilution of the warrant requirement. *Id.* (quoting *Kahn*, 415 U.S. at 154-55).

153 *See id.* 436 U.S. at 137 (positing that courts may "undertake[ ] an objective assessment of an officer's actions in light of the facts and circumstances then known to him"); *Kahn*, 415 U.S. at 155 (determining that particularity in identifying parties in an interception order is not necessary unless parties are known); *Donovan*, 429 U.S. at 439 (reasoning that failure to identify parties in interception application, order, or notice is not a fatal flaw and does not preclude admissibility of intercepted communications); *Chavez*, 416 U.S. at 574-75 (stating that violations of Title III requirements do not render interceptions unlawful or inadmissible).

Demonstrating that it is not blind to the damage it has dealt to the Title III safeguards, the *Chavez* Court opined that "strict adherence by the Government to the

Even when limited to legitimate criminal investigations, wiretaps inevitably affect many innocent people as well as criminals.[154] Wiretaps in the modern communications world intercept more kinds and quantities of information over telephone lines than ever before.[155] Because key escrow gives the government the keys to unlock any supposedly secure electronic communication, the Clipper chip offers an unparalleled potential for governmental abuse of access to the information highway.[156] In the aftermath of cases such as *Scott v. United States*,[157] no protection against government intrusions exists other than a blind faith in the government's trustworthiness.[158]

The primary law enforcement argument in support of the Clipper chip is a nightmarish scenario of an impenetrable criminal cyberfortress, an electronic network dedicated to terrorism, child pornography, organized crime, and drugs.[159] Law enforcement

---

provisions of Title III would nonetheless be more in keeping with the responsibilities Congress has imposed upon it when authority to engage in wiretapping or electronic surveillance is sought." *Chavez*, 416 U.S. at 580. The *Donovan* Court echoed this sentiment. *Donovan*, 429 U.S. at 440 (quoting *Chavez*, 416 U.S. at 580).

154 *See Scott*, 436 U.S. at 132 (demonstrating that only 40% of intercepted conversations were related to the investigation); *supra* note 68 (discussing the number of people and conversations affected by wiretaps).

155 *See* Meyer & Glick, *supra* note 148, at 38 (quotation omitted). Armed with the Clipper chip, government agents could intercept not only telephone conversations and computer files, but also home shopping transactions, credit information, bank records, and personal data. *Id.* (quotation omitted). Telephone lines may soon carry interactive television, offering services from video malls to movies on demand. Evan Schwartz, *Ray Smith: The I-way, My Way*, WIRED, Feb. 1995, at 113, 114. As the so-called "information super-highway" develops, consumers will demand an even greater variety of services. *See* Kevin Kelly, *What People Really Want on the Net*, WIRED, Feb. 1995, at 48, 48 (contending that people are going to use the infobahn for "[s]ex, gambling, fun with role playing, sports, and chat groups. Oh yeah, and every now and then they'll take a few minutes to vote").

156 *See* Nick Gillespie, *Blunder Road*, REASON, Apr. 1994, at 6, 7 (arguing that the Clipper chip poses a threat to democratic government). The Clipper chip could produce a chilling effect on the "free flow of information that is the precondition of all democratic societies." *Id.*

157 *See Scott*, 436 U.S. at 137 (proclaiming that the minimization requirement should be evaluated objectively without regard to the investigating agents' subjective intent); *Donovan*, 429 U.S. at 439 (holding that failure to comply with Title III requirements does not render evidence inadmissible); *Chavez*, 416 U.S. at 574-75 (concluding that interceptions violative of Title III requirements are not necessarily unlawful); *Kahn*, 415 U.S. at 155 (determining that a wiretap need not be limited to parties named in the interception order).

158 *See* Godwin, *Privacy*, *supra* note 142, at 41 (stating that the Clipper chip requires individuals to trust the government).

159 Levy, *supra* note 4, at 48. Law enforcement officials hypothesize that criminals will use unregulated encryption to protect their activities, thereby hiding behind impenetrable digital walls. *Id.* Government officials suggest that the criminal exploitation of encryption threatens the legal process itself. *Id.*

agencies claim that unless the Clipper chip is adopted to guarantee the ability to wiretap, uncontrolled encryption technology inevitably will lead to such a network.[160]

The Clipper chip is the linchpin in a government strategy to limit the extent to which private citizens and businesses can protect themselves. Strict export controls decrease the availability and dilute the potency of strong encryption technology.[161] By limiting the development of digital communications networks, the Digital Telephony Act seeks to maintain the status quo in a field that witnesses fundamental change in monthly cycles.[162] The Clipper chip, which on its face offers an encryption standard balanced by law enforcement's interests, in fact dictates how information is kept private.[163] The combination of these strategies is an obvious effort to increase, or at the very least maintain, the government's ability to eavesdrop on communications.

This initiative must be placed in the context of the balance between law enforcement and privacy.[164] The concept of privacy, namely the protection from government intrusions into the home, has taken on greater significance as information has become more valuable as a commodity. Encryption technology provides absolute protection of this wealth of information. Law enforcement's interest in accessing this information is defeated by encryption.[165] Conversely, the Clipper chip allows the government to control the extent to which information and communication may be kept private.[166] By giving the government control of privacy, that delicate

---

160 *Id. But see supra* note 142 and accompanying text (arguing that because Clipper is not mandatory, criminals are not obligated to use it). Even if a criminal had a Clipper chip system, the technology does not prevent the use of a second program to double-encrypt information. *House Hearing, supra* note 11, at 56 (statement of Jerry Berman, Executive Director, Electronic Frontier Foundation).

161 *See supra* notes 115-17 and accompanying text (discussing the law of export controls and its effect on encryption technology). Generally, export controls cost American businesses billions of dollars, undermine their competitiveness, and force the marketing of inferior encryption programs. Aley, *supra* note 117, at 30.

162 *See supra* notes 119-24 and accompanying text (discussing the Digital Telephony Act). The Digital Telephony Act forces telecommunication carriers to redesign their digital systems to facilitate eavesdropping. *See* Godwin, *Government, supra* note 122, at 93.

163 *See* Gillespie, *supra* note 156, at 7 (quotation omitted) (reasoning that the government's adoption of the Clipper chip is an attempt to undermine the spread of high-quality commercial encryption).

164 *See* Andrews, *supra* note 9, at 48 (quoting Vice President Al Gore's assertion that the Clipper chip balances encryption and law enforcement).

165 *House Hearing, supra* note 11, at 13 (statement of James Kallstrom, Special Agent in Charge, F.B.I.).

166 *See* Gillespie, *supra* note 156, at 7 ("The costs of 'insuring' the needs of law

balance is destroyed. The country is faced with an ultimate choice: genuine communications security or complete law enforcement access to information.

The tension between wiretapping and privacy may be viewed in terms of simple illegality. The interception of electronic information is not only illegal, it is also an invasion of privacy and abhorrent to the public interest.[167] Judicially authorized law enforcement interceptions are an exception to that rule. With the Clipper chip, privacy is the exception.

VI. CONCLUSION

While the Clipper Chip itself may not present a catastrophic threat to the Fourth Amendment, the sobering implications of the government strategy are only now being recognized.[168] The underlying premise of judicially authorized electronic eavesdropping is one of balance between the needs of law enforcement and the requirements of the Fourth Amendment.[169] Wiretapping has consistently been characterized as a public evil, yet it has been tolerated,

---

enforcement and national security are typically paid by selling off personal liberties.").

167 *See* S. REP. NO. 541, 99th Cong., 2d Sess. 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559. The legislative history of the ECPA stressed that

> the law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

Id.; *see also* S. REP. NO. 1097, 90th Cong., 2d Sess. 69 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2156 (emphasizing the need for national legislation to protect privacy rights); Berger v. New York, 388 U.S. 41, 45 (1967) (citation omitted) ("Eavesdropping is an ancient practice which at common law was condemned as a nuisance."); *Berger*, 388 U.S. at 64 (Douglas, J., concurring) (citations omitted) (articulating an "overriding objection to electronic surveillance, *viz.*, that it is a search for 'mere evidence' which . . . is a violation of the Fourth and Fifth Amendments, no matter with what nicety and precision a warrant may be drawn"); Katz v. United States, 389 U.S. 347, 359 (1967) (quotation omitted) (holding that antecedent justification is a "constitutional precondition" to the government's use of electronic eavesdropping).

168 *See House Hearing*, *supra* note 11, at 57 (statement of Jerry Berman, Executive Director, Electronic Frontier Foundation). Mr. Berman described the government strategy as "hovering over the information highway, an administration which wants to design and set standards which may inhibit the growth of that highway, threaten privacy, and impair international competitiveness." *Id.* Further, "the problem of accommodating the information needs of law enforcement in a way that preserves privacy rights will become more severe." *Id.* at 1 (statement of Rep. Tim Valentine, Chairman of the Subcommittee).

169 *Id.* Representative Valentine enunciated that "[t]herein lies the dilemma, what is the proper balance between the needs of law enforcement and the rights of citizens under the Fourth Amendment of the Constitution." *Id.*

within limitations, in the interests of public welfare and safety.[170] Aside from the particularity requirements imposed by common law and by statute, the most compelling protection against abuses in authorized interceptions has been the minimization requirement. Despite the Supreme Court's gradual erosion of the minimization standard, it remains the most potent barrier to increasing government access to private electronic data.

As technology has advanced, the range and depth of information carried over the nation's communications network has increased exponentially.[171] The government's use of wiretapping as a method of accessing information carried over the telephone lines was originally intended to be a limited tool, a last resort in the investigative process.[172] The Clipper chip and accompanying technologies and initiatives create the potential for eavesdropping to become the first step rather than the last resort. The balance between the Fourth Amendment and law enforcement has been fundamentally altered by advancing technologies.

Since the adoption of Title III in 1968, the Court has consistently interpreted constitutional and statutory safeguards on wiretapping in favor of law enforcement.[173] The government's adoption of the Clipper chip, combined with policies such as strict export license controls and the Digital Telephony Act, shift the advantage of technology to law enforcement and away from private security. Acceptance of these proposals requires citizens to trust the government to protect their privacy interests and to ignore the potential for abuse. The protection of these rights is not the duty of the government, but of the individual, and it is in turn the Judiciary's duty to balance the competing interests. It is time to reconsider this balance. Modern technology may require an absolute choice between privacy and law enforcement—who should hold the keys to information communication? Since 1968 the weight of

170 *See, e.g., Berger*, 388 U.S. at 62-63 (quotations omitted) (recognizing the necessity of wiretapping, despite its threat to liberty).

171 *See* Hellman, *supra* note 2, at 28, 29 (calculating the amount of information carried over the Internet).

172 *House Hearing, supra* note 11, at 10 (statement of James Kallstrom, Special Agent in Charge, F.B.I.).

173 *See* Theodore S. Basik, Note, 9 U. BALT. L. REV. 308, 341 (1980) (asserting that "the Court has made a policy decision favoring the governmental interest in law enforcement over the citizen's right to privacy").

the law has favored law enforcement. Wiretapping and other forms of electronic surveillance were intended to be tools limited in power and scope, not merely in number.[174] This basic proposition should be reasserted.

Christopher E. Torkelson†

174 *See House Hearing, supra* note 11, at 10 (statement of James Kallstrom, Special Agent in Charge, F.B.I.) (noting that Title III "permits electronic surveillance only for serious felony offenses and only when other investigative techniques will not work or are too dangerous.").

† Christopher Torkelson can be reached on the Internet at: torkelch@lanmail.shu.edu.