

comment

CHOPPY WATERS IN THE SURVEILLANCE DATA STREAM: THE CLIPPER SCHEME AND THE PARTICULARITY CLAUSE

Mark I. Koffsky †

Table of Contents

I. Introduction 131

II. The Clipper Scheme: An Effort To Maintain The Integrity Of Electronic Surveillance 133

A. The Current Proposal: "Optional Clipper" 133

B. A Hypothetical Extension: "Mandatory Clipper" 136

III. The Particularity Clause: Limiting The Scope Of An Electronic Surveillance 137

A. Particularity Clause Requirements For A Valid Electronic Surveillance 137

B. An Example: Particularity Clause Analysis of Title III 139

IV. The Particularity Clause As Applied To Mandatory Clipper 142

A. The Katz Analysis: Evaluating the Conduct of the Surveying Officers 143

B. The Berger Analysis: Evaluating the Mechanism That Enables the Surveillance 144

V. Conclusion 147

I. Introduction

The scene is a local police precinct. After obtaining proper authorization, the police establish a wiretap vital to their ongoing investigation of a suspected drug kingpin. The call is placed, the police listen intently, but they only hear garbled noise—the suspect is using a telephone equipped with encryption technology. Upon realizing that the sophisticated encryption scheme cannot be broken by even the most advanced computers, the police abandon their efforts. Their inability to decipher the encryption scheme has severely obstructed their ongoing investigation.

As these incidents grow in number, the Federal Government and law enforcement agencies become increasingly concerned with the obstruction imposed by encryption, both of voice and data. Any desire to remedy this problem, however, is tempered by the recognition that data encryption telephones are used primarily by businesses and citizens seeking to prevent others from listening to their conversations.¹ To accommodate law enforcement goals without compromising legitimate encryption needs, the Federal Government is considering using a mandatory Clipper scheme. A mandatory Clipper scheme would prohibit the use of all forms of private data encryption technology in telephones and require that those wishing to use data encryption devices use only authorized equipment. The authorized equipment would provide secure telephone conversations to thwart private eavesdroppers while enabling law enforcement officers to decrypt intercepted conversations using special computer keys. As a safeguard, law enforcement officials could only acquire the computer keys after first obtaining legal authorization for the electronic surveillance.

This Comment argues that a mandatory Clipper scheme violates the Fourth Amendment requirement that searches be conducted with

sufficient particularly.² Part II describes the current conflict between the proliferation of data encryption technology and electronic surveillance efforts by law enforcement officials, and postulates a Federal Government sponsored mandatory Clipper scheme as a solution. Part III presents the two-part evaluation currently used by the judiciary to evaluate the propriety of an electronic surveillance under the Particularity Clause: examining first the ordinance enabling the surveillance, and second the conduct of the officers executing the surveillance. Part IV argues that although the officers executing a surveillance under a mandatory Clipper scheme can act within the dictates of the Particularity Clause, courts should find that a mandatory Clipper scheme, on its face, violates the Particularity Clause.

II. The Clipper Scheme: An Effort To Maintain The Integrity Of Electronic Surveillance

A. The Current Proposal: "Optional Clipper"

In use for millennia for military³ and civilian purposes, data encryption is the process by which a message is sent in cryptic form to a recipient who, in turn, decodes the message with a "key." These keys can be as diverse as a letter substitution table or a computer program. Julius Caesar used a code where each letter was replaced by the third later letter in the Latin alphabet.⁴ In a perfect encryption scheme, no one other than the intended recipient of a message can decode, and therefore understand, the contents of the message.

Currently, consumers can purchase, from private parties, special telephones equipped with data encryption technology⁵ so advanced that eavesdroppers cannot understand conversations spoken on these telephones.⁶ The same encryption technology, however, can be used to shield criminals from Government surveillance since law enforcement officials engaged in authorized electronic surveillance cannot understand encrypted conversations.⁷ The recent increase in electronic surveillance by Government officials only exacerbates this problem.⁸

To resolve this quandary, the Clinton administration introduced the Clipper Chip initiative on April 16, 1993. The briefing by the White House proposing the Clipper initiative included the following: "While encryption technology can help Americans protect business secrets and unauthorized release of personal information, it also can be used by terrorists, drug dealers, and other criminals."⁹

The Clipper initiative envisions the use of a government manufactured computer chip to encrypt telephone signals.¹⁰ The resulting encryption would be highly effective because the chip's encryption algorithm is more secure than any data encryption technology currently available,¹¹ thereby providing effective protection from private citizens eavesdropping on each other. Thus, Clipper would protect legitimate business encryption needs while allowing access for authorized law enforcement officials.¹²

To insure that law enforcement officials will not abuse the Clipper initiative, the initiative requires that the computer key for each Clipper chip be split in half and housed in repositories maintained by two separate government agencies.¹³ Before obtaining these half-keys, law enforcement officials must obtain proper authorization for an electronic surveillance. After obtaining proper authorization and encountering a Clipper encrypted message, law enforcement officials obtain the Clipper chip's unique serial number from the intercepted transmission. The law enforcement officials then present this serial number and a copy of the electronic surveillance authorization to both escrow agencies, each of which would release its half of the decryption key for that chip.¹⁴ The officials can then combine the two half-keys into a whole key, allowing decryption of the intercepted conversation.¹⁵

B. A Hypothetical Extension: "Mandatory Clipper"

The actual Clipper initiative is not yet mandatory, but only a suggestion by the Federal Government as to how telecommunications companies should direct their technological development. The current Clipper thus suggests that telephone manufacturers use the Clipper chip, but it does not require them to do so. Since the ultimate effectiveness of the Clipper initiative requires widespread use of the Clipper chip by the telephone manufacturers, however, it is likely that the Government will eventually *require* telephone manufacturers to use the Clipper chip.¹⁶

The analysis in this Comment is based on the assumption that the Federal Government will soon take the Clipper initiative one step further and mandate that Clipper be the *sole* encryption technology used. To maintain clarity, this Comment will refer to the current, optional Clipper approach as "optional Clipper" and the hypothetical, mandatory Clipper approach as "mandatory Clipper."

Similar to other Federal agencies overseeing technology,¹⁷ mandatory Clipper would authorize an administrative body, the "Clipper Commission," to promulgate the mandatory standards in data encryption technology. As a key part of this, the Clipper Commission would require all publicly sold telephones containing data encryption devices to only use a Government manufactured computer

chip.¹⁸ Thus, mandatory Clipper redirects the evolution of telecommunications technology in order to accommodate the needs of law enforcement officials. All other aspects of mandatory Clipper would be the same as for optional Clipper.¹⁹

III. The Particularity Clause: Limiting The Scope Of An Electronic Surveillance

Electronic surveillance must conform to the Fourth Amendment requirement that search warrants "particularly describ[e] the place to be searched, and the persons or things to be seized."²⁰ Part A reviews the Supreme Court cases *Berger v. New York*²¹ and *Katz v. United States*²², which jointly establish the criteria necessary for an electronic surveillance to be valid under the Particularity Clause. Part B uses the current federal electronic surveillance statute, Title III, as an example of how the legal criteria apply to electronic surveillance similar to mandatory Clipper.

A. Particularity Clause Requirements For A Valid Electronic Surveillance

The Framers incorporated the Particularity Clause into the Fourth Amendment to counter the fear of a general warrant used against the colonists by the English crown.²³ British officials obtained general warrants using writs of assistance empowering them, at their discretion, to search suspected places for smuggled goods placing the liberty of every man in the hands of every officer.²⁴ The Particularity Clause requires a warrant to specify the exact nature of a search in order to preclude any independent discretion on the part of the executing officer.²⁵ This requirement is designed to curtail potential abuse that may result from an officer being allowed to conduct a search with unbridled discretion. If a warrant is issued in violation of the Particularity Clause, the ensuing search is invalid even if the officers actually exercise proper restraint in executing their search.²⁶

In 1967, the Supreme Court defined the criteria necessary for electronic surveillance to be valid under the Particularity Clause in *Berger v. New York*²⁷ and *Katz v. United States*.²⁸ In *Berger*, the Supreme Court reviewed New York's electronic surveillance statute which allowed a judge to issue an *ex parte* sixty day authorization for electronic surveillance on the basis of a law enforcement official's testimony that the surveillance might reasonably produce evidence of a crime.²⁹ Although the statute required that law enforcement officials "particularly describ[e] the person or persons whose communications, conversations or discussions are to be overheard"³⁰ before a warrant could be issued, the Court found the statute to be inconsistent with the Particularity Clause. For example, the Court found fault with the statute's failure to require the officer to describe the type of conversations sought and thus allowing a general interception of all conversations without sufficient showing of probable cause. Additionally, an unlimited sixty-day authorization for electronic surveillance constituted an impermissibly broad license for continuous surveillance of all conversations.³¹ The significance of this decision is that the Court did not merely exclude the evidence that had been obtained; instead, the Court struck down the statute, itself, as violating the Particularity Clause.³²

In *Katz*, the Federal Government introduced evidence at trial that had been obtained from a properly authorized surveillance device placed outside of a public telephone booth³³ that recorded the defendant's conversations within the booth.³⁴ The Court found that three requirements of the Particularity Clause had been satisfied by the search. First, the Federal agents had sufficient probable cause that the suspect was using the telephone for illegal activity before undertaking the surveillance. Second, the agents limited their surveillance in scope and duration to the specific purpose of establishing the contents of the suspect's calls. Third, the agents only listened to the suspect's calls and exercised great effort not to listen to other's calls made from the phone booth.³⁵ Nevertheless, the Court ruled that the surveillance was unconstitutional because no judge or magistrate had overseen the procedures of the Government officials.³⁶

Berger and *Katz* together reveal the criteria necessary for an electronic surveillance to be valid under the Particularity Clause. *Berger* requires that the actual statute enabling the electronic surveillance must provide significant limitation on the scope of each surveillance. Under *Berger*, the Court used the Particularity Clause to invalidate an electronic surveillance statute based on the overly broad elements found within the statute. *Katz* focuses on what officers executing an electronic surveillance must do: have probable cause to execute the surveillance, make an effort to limit interceptions only to pertinent conversations and obtain prior independent judicial overview. In sum, these two cases together establish complementary approaches in the evaluation of electronic surveillance under the Particularity Clause: *Berger* reviews the statute that authorizes the surveillance whereas *Katz* concentrates on the conduct of the officers conducting the surveillance.

B. An Example: Particularity Clause Analysis of Title III

To determine how courts might evaluate mandatory Clipper, it is useful to examine how courts have analyzed the current Federal electronic surveillance statute, Title III.³⁷ To ensure that the statute, itself, satisfied *Berger*, Congress included restrictions within Title III that limited the scope and availability of electronic surveillance. Once law enforcement officials obtain a valid electronic

surveillance authorization,³⁸ Title III requires that they diligently refrain from listening to irrelevant conversations.³⁹ Title III also requires a law enforcement official to show probable cause that the suspect is involved with the commission of a crime and that the surveillance will obtain communications concerning the crime to the judge issuing a surveillance authorization.⁴⁰

Although Congress sought to ensure that Title III satisfied *Berger*,⁴¹ four defendants challenged the statute in *United States v. Cox*.⁴² The court found that Title III fulfilled nine criteria listed in *Berger*.⁴³ The court noted that the only portion of Title III that could be seriously questioned as failing the rigors of *Berger* is the provision allowing the surveillance orders to last thirty days.⁴⁴ The court determined that, having fulfilled each of the procedural safeguards mentioned in *Berger*, Title III is not rendered unconstitutional solely because it authorizes wiretaps which may last several days and encompass multiple conversations.⁴⁵

While *Berger* applies to the statute enabling the electronic surveillance, *Katz* applies to the conduct of the law enforcement officials. By the directive of *Katz*, the judicial branch must review the viability of the probable cause presented by the law enforcement officials.⁴⁶ The requirement of *Katz* that officers limit the scope of their surveillance, however, cannot be judged until after the surveillance has been completed. The Particularity Clause thus requires independent judicial review after each surveillance to insure that its requirements were actually met. This review is triggered when a defendant seeks to suppress the admission of evidence obtained from a Title III surveillance.

In *Scott v. United States*,⁴⁷ the Supreme Court analogized from other Fourth Amendment cases⁴⁸ and held that an objective standard is required to determine if the requirements of the Particularity Clause have been met during a given electronic surveillance.⁴⁹ This holding renders irrelevant the mindset of the officer engaged in the surveillance.⁵⁰ If a court finds that an objective violation of the Particularity Clause occurred, the exclusionary rule prevents the admission at trial of any evidence obtained from that electronic surveillance.⁵¹

IV. The Particularity Clause As Applied To Mandatory Clipper

Courts will employ the dual approach of *Berger* and *Katz* to evaluate the propriety of the Clipper scheme under the Particularity Clause. Mandatory Clipper satisfies *Katz* because the Clipper Commission can insure that the safeguards required by *Katz* will be present in mandatory Clipper. Nevertheless, courts should use *Berger* and its progeny as precedent to invalidate the Clipper scheme because of its intrusive and permanent nature.

A. The *Katz* Analysis: Evaluating the Conduct of the Surveying Officers

Similar to current Title III electronic searches, a search under mandatory Clipper presents unique difficulties under the Particularity Clause when compared to conventional searches. In a conventional search, the articles subject to search or seizure already exist. The executing officer must simply retrieve the objects in accordance with the specifications of the authorization,⁵² thus limiting the discretion of the executing officer as required by the Particularity Clause. Even the most clearly written Clipper authorization, however, cannot overcome the fact that the target of a Clipper surveillance—a future conversation—may never occur.⁵³ An officer executing a Clipper surveillance must exercise discretion in what conversations to overhear, the very type of discretion prohibited by the Particularity Clause.⁵⁴

As discussed above,⁵⁵ however, courts have allowed electronic surveillance to pass muster under the Particularity Clause despite these problems. Because the requirements for an officer's conduct under mandatory Clipper would likely be similar to that for current Title III searches, the courts will probably uphold mandatory Clipper under the requirements of the Particularity Clause as delineated in *Katz*.⁵⁶

For example, *Katz* requires a showing of probable cause in order to obtain authorization for an electronic surveillance. The Clipper Commission would satisfy this directive by allowing officers to obtain a surveillance authorization only where probable cause exists. The surveillance authorization would be a necessary requirement before the officers could access the computer keys needed for decryption. The Clipper Commission would also satisfy the *Katz* requirement that officers limit the scope of their surveillance by mandating that officers conducting Clipper surveillance limit interceptions to pertinent conversations.

Katz also requires an independent judicial review after each surveillance. To fulfill this requirement, the Clipper Commission could explicitly grant the courts the right to undertake ex post evaluation of a Clipper search when the defendant so desires. As explained earlier, any such review would likely be an objective evaluation without a subjective inquiry into the motives of the surveying officers. If the court finds the officers violated the Particularity Clause, the exclusionary rule would prohibit the introduction of evidence obtained from the surveillance.⁵⁷

B. The *Berger* Analysis: Evaluating the Mechanism That Enables the Surveillance

The direction of inquiry under *Berger* differs from that under *Katz*. While a *Katz* inquiry focuses on the implementation of the mechanism⁵⁸ that enables the electronic surveillance, a *Berger* inquiry dissects the propriety of the enabling mechanism, itself. To understand how the courts might apply *Berger* to mandatory Clipper, it may be useful to examine how courts have applied the Particularity Clause in other situations.

Because it would be impossible to describe every item targeted in a search, the courts has made allowances for the specificity required by the Particularity Clause. In *Andresen v. Maryland*,⁵⁹ the Supreme Court reviewed a search warrant that contained the phrase "together with other fruits, instrumentalities and evidence of crime at this [time] unknown," when the subject of the search was incriminating business papers.⁶⁰ The defendant argued that the phrase allowed the police too much discretion in choosing which papers to seize, thus creating a general warrant forbidden under the Particularity Clause. The Court disagreed, choosing to read this phrase as an extension of the antecedent text which authorized the police to seize a set of papers.⁶¹ In upholding the warrant, the Court declared that the defendant could not use the defense of a general warrant to hide behind the complex nature of the crime.⁶²

The lower courts extended this notion by upholding broadly written warrants authorizing seizures related to suspect items. For example, the Second Circuit found no violation of the Clause when a law enforcement officer exercised minimal discretion over which items to search under a warrant that contained an incomplete list of drug items.⁶³ Similar holdings from circuit courts found broadly written search warrants not to violate the Particularity Clause when the subjects of the searches were tax documents,⁶⁴ burglary tools,⁶⁵ motor vehicles⁶⁶ and firearms.⁶⁷

In some cases, however, the courts have not been willing to overlook broadly written warrants. In *Stanford v. Texas*,⁶⁸ the Supreme Court struck down the validity of a search warrant authorizing officers to seize all the papers in the home of a suspected member of the Communist Party.⁶⁹ The Court held that when the targets of a warrant are books and the basis of the seizure is the ideas which the contain, the Particularity Clause must be applied with the "most scrupulous exactitude."⁷⁰ In other cases, courts have invalidated warrants as too general when the objectives of the search were the books and papers of a school suspected of defrauding the Federal Government,⁷¹ electronic tapes suspected of copyright abuse⁷² and printed seditious matter.⁷³

These decisions reveal a judicial tendency to apply the Particularity Clause with differing degrees of scrutiny based on factors other than just the language of the search warrant.⁷⁴ The unique features of mandatory Clipper require that the Particularity Clause be applied with especially strict scrutiny.

One unique feature of mandatory Clipper is that it requires implantation of a computer chip into an entire class of telephones only because these telephones may someday be used to commit a crime. The anticipatory approach undercuts the probable cause needed for any search—a reasonable ground of suspicion supported by circumstances sufficiently strong to warrant a reasonably cautious and prudent person in believing that a crime has been or is being committed,⁷⁵ but not on the belief that a crime will be committed.⁷⁶

This application of probable cause in the *Berger* analysis differs from that required by *Katz*. As explained earlier, *Katz* requires a judicial overview of each warrant to insure that probable cause exists for the specific search at issue.⁷⁷ *Berger*, on the other hand, focuses on aspects of the statute that would almost certainly later lead to a violation of the probable cause requirement. In *Berger*, the Court found that the New York statute, by generally allowing interception of all conversations, would authorize search warrants even where sufficient probable cause did not exist.⁷⁸ Similarly, mandatory Clipper fails under *Berger* because it implants the Clipper chip in anticipation of future surveillance without the need to show any probable cause at the time of implantation. Therefore, any search warrant obtained under mandatory Clipper would be a result of this unjustified initial implantation.⁷⁹

Another unique feature of mandatory Clipper is its permanence. In a conventional search as well as a Title III electronic surveillance, any equipment used by a law enforcement organization is removed after the search is completed. In mandatory Clipper, however, the Clipper chip remains in the telephone indefinitely.⁸⁰ Thus, whereas a conventional search is directed to one specified area and whereas a Title III electronic surveillance is similarly limited in scope,⁸¹ mandatory Clipper is directed to an entire class of telephones. Courts should consider this permanent intrusion by the Federal Government into the telephone—a device not inherently linked with criminal activity⁸² where citizens expect their conversations⁸³ will be kept private⁸³—when evaluating its propriety under the Particularity Clause.⁸⁴

V. Conclusion

The mere fact that Title III surveillance has withstood examination under *Berger* does not require the same result for mandatory Clipper surveillance. Applying a *Berger* analysis, the courts should invalidate mandatory Clipper because of the totality of problems caused by its implementation. A computer chip—a device required for any successful search—is placed into an entire class of telephones in the anticipation of a future crime. Moreover, an authorization for a mandatory Clipper surveillance may never have sufficient probable cause since the authorization would be partially based on an unwarranted assumption that a crime might be committed. Finally, mandatory Clipper's unprecedented, permanent intrusion into an entire class of telephones is at odds with the intent of the Particularity Clause to limit the scope of an authorized search.⁸⁵ In sum, it is the duty of the courts to examine the Clipper scheme critically to insure that the protections of the Fourth Amendment remain unwavering from the Federal Government's attempts to narrow them in the name of effective law enforcement.⁸⁶

Ultimately, the path the judiciary chooses when deciding the fate of mandatory Clipper will depend on the evaluation of the public policy issues presented by the scheme. Without mandatory Clipper, it is conceivable that electronic surveillance will cease to be an effective tool for law enforcement.⁸⁷ As a result, the abolition of Clipper might lead to fewer arrests and convictions. It also might, however, force law enforcement organizations to redirect their efforts into other, less intrusive means.

Over sixty years ago, Justice Brandeis warned: "The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping."⁸⁸ Our next millennium will see technology continue to proliferate into all areas of daily life. One heralded example, the "information superhighway," will enable information exchange on a massive scale.⁸⁹ If the courts uphold mandatory Clipper, it would establish the precedent that the Federal Government has the right to direct the development of technology in a manner amenable to its own interests. The judiciary should preclude this governmental intervention by invalidating mandatory Clipper.

† 1994 Mark I. Koffsky.

† J.D. Candidate 1995, Columbia University School of Law; B.S. Electrical Engineering 1992, Columbia University School of Engineering; B.A. Physics 1992, Yeshiva University.

1. Keeping voice and data lines secure from industrial espionage costs large corporations and small businesses billions of dollars per year. *See* Stephen M. Williams, *Companies Compile Dossiers on Rivals*, THE HARTFORD COURANT, June 7, 1993, at 1.

2. The Fourth Amendment to the Constitution of the United States provides:

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 (emphasis added)[emphasized portion hereinafter the Particularity Clause].

3. Encryption technology has often been associated with the military. Even today, the U.S. Munitions List is the repository for encryption regulation. *See* 22 C.F.R. § 121.1(b)(1) (1992).

4. *See* James L. Massey, *Contemporary Cryptology: An Introduction*, in CONTEMPORARY CRYPTOLOGY 3, 6 (Gustavus J. Simmons ed., 1992). "COLUMBIA" in Caesar's code would become "FROXPELD". *See also* Ernst L. Leiss, PRINCIPLES OF DATA SECURITY 178-79 (1982)(discussing the mathematical theory behind the dual key algorithm, one of the most secure encryption schemes available).

5. *See* John Eckhouse, *New Phones Keep Trade Secrets Safe*, S.F. CHRON., July 9, 1993, at E1.

6. The RSA public key algorithm is one of the best-known data encryption systems. It would take a computer that performs 1 trillion operations per second approximately 1000 years to break a standard RSA encryption. *See* James Nechvatal, *Public Key Cryptography*, in CONTEMPORARY CRYPTOLOGY 177, 207-08 (Gustavus J. Simmons ed., 1992).

The possibility that an encryption scheme can be so effective that it cannot be decrypted at all can be better understood by analyzing

properties of one-way mathematical functions. In general, a mathematical function takes a parameter, x , and yields a result, y . For example the cube function can be expressed as:

$$y = x^3$$

The inverse of the function takes the result, y , and yields the parameter x . The inverse of the above equation, the cube root function, is:



Functions that are easier to compute in their normal form than in their inverse form are known as one-way functions. The cube function is such a function because it is easier to compute the cube of 3 than the cube root of 27.

To illustrate by hypothetical, S wants to send R a message using the cube code. The message is the number 12.1 (assume the message is in numerical form). S encrypts the message by using the cube function producing the number 1771.561 and sends that number to R . Assume further that the message is intercepted by Z and Z knows that the encryption was accomplished via the cube function. Z will need to expend more effort to decrypt the message using the inverse of the cube function (i.e. the cube root function) than S did in encrypting the message. Obviously, Z will be able to decrypt the message by using a calculator or a cube root table. If S were to use a more complicated one-way mathematical function, Z would have more difficulty in decrypting the message even if Z knows the function. Effective encryption techniques take advantage of this fact. See Bob Metcalfe, *One-way Functions are the Key to Security*, INFOWORLD, Sept. 27, 1993, at 65.

7. James E. Kallstrom, the FBI's chief of investigation technology, commenting on the optional Clipper scheme, stated: "We feel we need these tools to do our job." John Mintz & John Schwartz, *Chipping Away at Privacy?*, WASH. POST, May 30, 1993, at H1. Kallstrom feared the consequences that might result if Clipper is not implemented. "I don't have a lot of dead bodies laying around here or dead children from an airplane explosion that we haven't been able to solve-yet." *Id.*

8. Each year, the Director of the Administrative Office of the United States Courts transmits a report to Congress summarizing the use of electronic surveillance by law enforcement officials in the past year. See 18 U.S.C. § 2519(3) (1988). 738 applications submitted for the authorization of electronic surveillance were approved in 1988. This represented a 10% increase over the approvals in 1987. See THE STATISTICAL ANALYSIS AND REPORTS DIVISION, ADMINISTRATIVE OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL OR ELECTRONIC COMMUNICATIONS (WIRETAP REPORT) FOR THE PERIOD JANUARY 1, 1988 TO DECEMBER 31, 1988 2 (1989).

9. Dee Dee Myers, Statement at The White House, April 16, 1993. Development of the Clipper initiative actually began during the Bush administration. The National Security Agency and the National Institute of Standards and Technology started development on Clipper in 1989. See Richard Lipkin, *Making the Calls in a New Era of Communication*, INSIGHT, Jul. 12, 1993, at 6.

10. The Federal Government has designated Mykotronx, a company located in Torrance, California, to manufacture the Clipper chips. See Dee Dee Myers, Statement at The White House, April 16, 1993 and attachments thereto.

11. Clipper employs the Skipjack algorithm which uses an 80-bit key, more powerful than the 56-bit key used by the popular Data Encryption Standard (DES) developed by IBM in 1976. See Dorothy E. Denning, *Cryptography, Clipper, and Capstone* (Draft of May 11, 1993), in THE THIRD CPSR CRYPTOGRAPHY AND PRIVACY CONFERENCE SOURCE BOOK (David Banisar & Marc Rotenberg eds. 1993), at 3-5. Skipjack is a classified algorithm developed by the National Security Agency. The secret nature of the Skipjack algorithm caused particular concern in the private sector because of the possibility that the National Security Agency had left a "trap door" in the Clipper chip. If present, the trap door would allow summary decryption of conversations without the need to obtain the necessary decryption keys from the repository agencies via a court authorization.

To allay these fears, the Federal Government invited five computer scientists to examine the classified algorithm in the summer of 1993. Although the scientists were forbidden to discuss their specific findings, they claimed no trap door exists in Clipper. See Robert L. Holtz, *Computer Code's Security Worries Privacy Watchdogs*, L.A. TIMES, Oct. 4, 1993, at A1.

12. The Clipper initiative proposal contains the following: "This new technology will help companies protect proprietary information, protect the privacy of personal phone conversations and prevent unauthorized release of data transmitted electronically. At the same time this technology preserves the ability of federal, state and local law enforcement agencies to intercept lawfully the phone conversations of criminals." Dee Dee Myers, Statement at The White House, April 16, 1993 and attachments thereto.

This statement reflects the Federal Government's desire to convince the public that it is striking the correct balance between the legitimate needs of law enforcement and the desires of private citizens to maintain the privacy of conversations.

13. The two repository agencies for the keys are the National Institute of Standards and Technology (NIST) and an as yet unnamed Treasury department division. *See* Sharon Fisher, *Who'll Hold Clipper Keys?*, COMMUNICATIONS WEEK, Sept. 27, 1993, at 35.

14. *See* Presentation of Raymond G. Kammer, Acting Director of the National Institute of Standards and Technology on a U.S. Technology Initiative for Secure Telephone Communications (April 16, 1993), in THE THIRD CPSR CRYPTOGRAPHY AND PRIVACY CONFERENCE (David Banisar and Marc Rotenberg, eds. 1993); Robert L. Holtz, *Demanding the Ability to Snoop*, L.A. TIMES, Oct. 3, 1993, at A1.

15. What remains unevaluated is why any criminal would use a telephone with a government installed computer chip that would enable the Government to listen to incriminating conversations. Optional Clipper does not address this question. Although this Comment will not address this issue, a possible response would be that criminals have used regular telephones for years even though those conversations can also be intercepted by the Government.

16. In fact, this approach has already been suggested by Clinton administration sources. "Administration sources said if the current plan doesn't enable the NSA and FBI to keep on top of the technology, then Clinton is prepared to introduce legislation to require use of its encryption technology, which is crackable by the NSA, and to ban use of the uncrackable gear." Mintz & Schwartz, *supra* note 7, at H1.

Discussing this hypothetical sidesteps the issue of at what point actions taken by the Federal Government constitute "state action." It is well settled that Fourth Amendment scrutiny only applies to such "state action." *See* *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921); *Honeycutt v. Aetna Insurance Co.*, 510 F.2d 340, 348 (7th Cir.), *cert. denied* 421 U.S. 1011 (1975).

17. *See, e.g.*, The Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724 (1988) (codified at 15 U.S.C. §§ 271 note, 272, 278g-3, 278g-4, 278h (1988)), 40 U.S.C. §§ 759, 759 note (1988)) (establishing, *inter alia*, a Computer System Security and Privacy Advisory Board to advise the Secretary of Commerce on security and privacy issues relating to Federal computer systems).

18. Telephone companies could, however, continue to sell non-encrypted telephones as before.

19. *See supra* Part II.A.

20. U.S. CONST. amend. IV.

21. 388 U.S. 41 (1967).

22. 389 U.S. 347 (1967).

23. *See* *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) ("By limiting the authorization to search to the specified areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."). *See also* *Entick v. Carrington*, 19 Howell's State Trials 1029, 1074 (Court of Common Pleas, Mich. Term: 6 George III, 1765) (refusing to recognize the validity of a general warrant used by messengers of the King).

24. *Boyd v. United States*, 116 U.S. 616, 625 (1886). *See also id.* at 624-630 (detailing the historical background as to why the Framers adopted the Fourth Amendment).

25. *See* *Marron v. United States*, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."); *United States v. Crozier*, 777 F.2d 1376, 1380 (9th Cir. 1985).

26. "[P]rosecutors and policemen simply cannot be asked to maintain the requisite neutrality with regard to their own investigation."

Coolidge v. New Hampshire, 403 U.S. 443, 450-51 (1971). "[T]he rights against unlawful search . . . and seizure are to be protected even if the same result might have been achieved in a lawful way." *Id.* (quoting *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920)). *See also* *United States v. George*, 975 F.2d 72, 75-76 (2d Cir. 1992) (holding that a warrant's general language could not be overcome by officer's affidavit that made clear that only evidence relating to the crime in question was seized).

27. 388 U.S. 41 (1967). *Berger* implicitly overruled *Olmstead v. United States*, 277 U.S. 438, 466 (1928), the first electronic surveillance case to reach the Supreme Court. *Berger*, 388 U.S. at 64 (Douglas, J. concurring). *Olmstead* held that electronic surveillance was not an intrusion into the home and therefore did not trigger Fourth Amendment scrutiny: "The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the scope of Fourth Amendment." *Olmstead*, 277 U.S. at 466.

28. 389 U.S. 347 (1967).

29. 1958 N.Y. Laws 1513-14 (repealed 1967). The current New York electronic surveillance statute is codified at N.Y. CRIM. PROC. LAW §§ 700.05-700.65 (McKinney 1984 & Supp. 1993).

30. 1958 N.Y. Laws 1513.

31. *Berger*, 388 U.S. at 58-60.

32. *Id.* at 63.

33. Before *Katz*, the legality of an electronic surveillance generally turned on the invasion of a constitutionally protected area. The Court had upheld the use of a recording device placed outside an office wall to record conversations within, *see Goldman v. United States*, 316 U.S. 129, 134-35 (1942), but held that installing a surveillance device that penetrated into a suspect's house was a violation of the Fourth Amendment. *See Silverman v. United States*, 365 U.S. 505, 509-11 (1961). Such areas of constitutional protection did not necessarily correspond to traditional notions of property. *See Warden, Maryland Penitentiary v. Hayden*, 387 U.S. 294, 304 (1967) (property interests do not control the right of the Government to search and seize under the Fourth Amendment); *Silverman*, 365 U.S. at 511 (1961) (no trespass under local property law necessary to encroach upon a constitutionally protected area).

34. *Katz*, 389 U.S. at 348.

35. *Id.* at 354.

36. *Id.* at 356-57.

37. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 218, Pub. L. No. 90-351 (codified at 18 U.S.C. §§ 2510-2521 (1988)) [hereinafter Title III]. Congress updated Title III in 1986 by amending the phrase "wire or oral communication" to "wire, oral or electronic communication" throughout the statute, 100 Stat. 1848, Pub. L. No. 99-508 (1986), in order to accommodate changing telecommunications technology. *See* S. REP. NO. 541, 99th Cong., 2d Sess. 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555. State agencies are subject to this statute as well as the law of their state. *See generally*, ABA Standards for Criminal Justice, app. at 2.75-2.78 (2d ed. 1980 & Supp. 1986) (comparing the Federal electronic surveillance law with many of their state counterparts including history of passage and differences in content). Because Clipper is a Federal initiative, this Comment will focus on the Federal electronic surveillance statute.

38. Each electronic surveillance authorization is valid only until the objective of the authorization has been fulfilled, or thirty days, whichever is earlier. *See* 18 U.S.C. § 2518(5). Judges can grant unlimited thirty day extensions until the purpose of the surveillance has been accomplished. *Id.* Nevertheless, the judge must include in his or her authorization order "a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained." 18 U.S.C. § 2518(4)(e).

39. 18 U.S.C. § 2518(5). *See United States v. Sisca*, 361 F. Supp. 735, 745 (S.D.N.Y. 1973), *aff'd*, 503 F.2d 1337 (2d Cir.), *cert. denied*, 419 U.S. 1008 (1974). Recognizing the difficulty in determining the relevance of every conversation at the beginning of a surveillance, courts permit Government officials to listen to all of the conversations on a surveyed telephone for a limited time enabling them to identify the speakers and determine their pertinence to the investigation. *See United States v. Gotti*, 771 F. Supp. 535,

550 (E.D.N.Y. 1991) (allowing spot checks at the beginning of all conversations throughout the surveillance period). These spot interceptions usually last from one to two minutes. *See* *United States v. Willis*, 890 F.2d 1099, 1102 (10th Cir. 1989); *United States v. Angiulo*, 847 F.2d 956, 978-80 (1st Cir. 1988). But they can often be longer without tainting the surveillance. *See, e.g., Salzman v. State*, 430 A.2d 847, 857 (Md. App. 1981) (ten minutes); *United States v. Hinton*, 543 F.2d 1002, 1012 (2d Cir.) (five minutes), *cert. denied sub nom. Carter v. United States*, 429 U.S. 980 (1976). Once the Government officials identify parties they are not authorized to overhear, a duty exists for the surveyors to refrain from monitoring calls involving those parties. *See United States v. Abascal*, 564 F.2d 821, 827 (9th Cir. 1977), *cert. denied sub nom. Frakes v. United States*, 435 U.S. 942 (1978). *See also* Clifford S. Fishman, *The "Minimization" Requirement in Electronic Surveillance: Title III, The Fourth Amendment and the Dread Scott Decision*, 28 AM. U. L. REV. 315, 326-29 (1979) (discussing procedures Government officials use to limit the interception of surveyed conversations).

40. 18 U.S.C. §§ 2518(3)(a)-(b). *But cf.* Fed. R. Crim. P. 41(c)(1) (requiring a higher standard of probable cause for a search warrant to be served during the nighttime than during the daytime.).

41. *See Berger*, 388 U.S. at 58-59; S. REP. NO. 1097, 90th Cong., 2d Sess. 102 reprinted in 1968 U.S.C.C.A.N. 2112, 2191.

42. 462 F.2d 1293 (8th Cir. 1972), *cert. denied*, 417 U.S. 918 (1974).

43. The nine requirements are:

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

Id. at 1302-1303. The following sections of Title III address respectively each of the above-enumerated criteria: (1) 18 U.S.C. § 2516; (2) §§ 2518(1)(f) and (2); (3) § 2518(1)(b)(i); (4) §§ 2518(1)(b)(iii), (4)(a) and (4)(b); (5) §§ 2518(1)(b)(iii) and (4)(c); (6) § 2518(6); (7) §§ 2518(1)(d), (4)(e) and (5); (8) §§ 2518(1)(c), (3)(c) and (8)(d); (9) §§ 2518(8)(a) and (8)(b). *See Cox*, 462 F.2d at 1303 n.14.

44. *See* 18 U.S.C. § 2518(5).

45. *Cox*, 462 F.2d at 1303. When faced with a similar issue one district court judge did not follow the *Cox* decision in affirming Title III's constitutionality. In *United States v. Whitaker*, 343 F. Supp. 358, 363-366 (E.D. Pa. 1972), *rev'd per curiam*, 474 F.2d 1246 (3d Cir.), *cert. denied*, 412 U.S. 953 (1973), the district court granted the defendant's motion to suppress evidence obtained via a Title III wiretap because the statute violated the Particularity Clause. "Title III permits the government to conduct lengthy continuous searches with great discretion in the hands of the executing officers, thus violating the Fourth Amendment's prohibition against general searches." *Id.* at 363. Although the court considered Title III superior to the New York surveillance statute struck down in *Berger*, the court justified its holding by noting Title III can authorize "continuous searches for months on end if a fresh showing of probable cause can be made once a month." *Id.* at 365. On appeal, the Third Circuit overturned the district court's ruling, stating that its holding in a previous case had definitively affirmed the constitutionality of Title III. *Whitaker*, 474 F.2d 1246, 1247 (3d Cir.) (per curiam), *cert. denied*, 412 U.S. 953 (1973). The previous case was *United States v. Cafero*, 473 F.2d 489 (3d Cir. 1973), *cert. denied sub nom. Carero v. United States*, 417 U.S. 918 (1974). Though no longer valid as precedent, the *Whitaker* district court opinion occupies a special place in history because of its disparity with an otherwise united judiciary holding Title III to be constitutional. *See, e.g., United States v. Leta*, 332 F. Supp. 1357, 1360-61 (M.D. Pa. 1971) (holding that a continuous thirty day wiretap was not offensive to Fourth Amendment because length of search was reasonable).

46. *See Katz*, 389 U.S. at 356-57.

47. 436 U.S. 128 (1978).

48. The Court, 436 U.S. at 137, cited *Terry v. Ohio*, 392 U.S. 1 (1968), where Chief Justice Warren, delivering the Opinion of the Court, wrote:

The scheme of the Fourth Amendment becomes meaningful only when it is assured that at some point the conduct of those charged with enforcing the laws can be subjected to the more detached, neutral scrutiny of a judge who must evaluate the reasonableness of a particular search or seizure in light of the particular circumstances. And in making that assessment it is imperative that the facts be judged against an objective standard: would the facts available to the officer at the moment of the seizure or the search warrant a man of reasonable caution in the belief "that the action taken was appropriate? Anything less would invite intrusions upon constitutionally guaranteed rights based on nothing more substantial than inarticulate hunches

Terry, 392 U.S. at 21-22 (citations omitted). The Court also cited, 436 U.S. at 138, *United States v. Robinson*, 414 U.S. 218 (1973) (permitting full bodied search of a defendant by an officer when probable cause existed that the suspect was operating a motor vehicle with a revoked license).

49. *Scott*, 436 U.S. at 136-37.

50. *Id.* at 138.

51. The Supreme Court ruled in *Weeks v. United States*, 232 U.S. 383, 398 (1914), that items obtained in violation of a suspect's Fourth Amendment rights could not be introduced into evidence at trial. In *Wolf v. Colorado*, 338 U.S. 25, 33 (1949), the Supreme Court ruled that the Fourth Amendment was applicable to the States via the Fourteenth Amendment, but that the exclusionary rule of *Weeks* was not a necessary component of the Amendment. Overruling *Wolf*, the Court held in *Mapp v. Ohio*, 367 U.S. 643, 654-55 (1961), that adherence to the exclusionary rule by the states was mandatory.

52. *But see Dalia v. United States*, 441 U.S. 238, 247-48 (1979) (stating that Fourth Amendment does not require an electronic surveillance authorization to explicitly permit breaking and entering into a suspect's home to install equipment necessary for the surveillance).

53. In arguing that electronic surveillance falls outside of the Fourth Amendment, Justice Black, dissenting in *Katz* stated:

[T]he language of the second [Particularity] clause indicates that the Amendment refers not only to something tangible so it can be seized but to something already in existence so it can be described. Yet the Court's interpretation would have the Amendment apply to overhearing future conversations which by their very nature are nonexistent until they take place. How can one 'describe' a future conversation, and, if one cannot, how can a magistrate issue a warrant to eavesdrop on one in the future? It is argued that information showing what is expected to be said is sufficient to limit the boundaries of what later can be admitted into evidence; but does such general information really meet the specific language of the Amendment which says 'particularly describing'?

Katz, at 365-66 (Black, J. dissenting). *See also United States v. Sklaroff*, 323 F. Supp. 296, 307 (S.D. Fla. 1971) ("It would be virtually impossible for the applicant for the order to predict in advance the exact language of a conversation which has not yet occurred.")

54. *See United States v. Weber*, 923 F.2d 1338, 1342 (9th Cir. 1990) (stating that particularity requirements require a warrant to be no broader than the probable cause on which it is based).

55. *See supra* Part III.B.

56. *See, e.g., United States v. Turner*, 528 F.2d 143, 154-55 (9th Cir.), *cert denied sub nom.*, *Grimes v. United States*, 423 U.S. 996 (1975) (upholding a Title III electronic surveillance warrant under the Particularity Clause because it was as precise as the circumstances permit).

57. In defending mandatory Clipper, the Government might further argue that citizens actually gain more protection from the threat of unauthorized wiretaps than existed before mandatory Clipper. Previously, Government officials could have easily set up an unauthorized electronic surveillance in secret. Under mandatory Clipper, Government officials can only violate citizen's constitutional rights by secretly obtaining the computer keys from the repository government agencies and executing an illegal surveillance. This additional step might serve as an added deterrent to government agencies contemplating an illegal electronic surveillance because of the additional paper trail. However, if mandatory Clipper contains a "back door" (a secret entry point or password known to only a few people) similar to one suspected to exist in optional Clipper, there would be nothing to prevent opportunistic Federal agencies from executing an illegal Clipper surveillance. *See supra* note 11.

Courts may ignore this line of argument entirely as the potential abuse of a power has been held to be irrelevant when determining whether the actual exercise of the power is valid under the Constitution. *See* *Bailey v. Richardson*, 182 F.2d 46, 62 (D.C. Cir. 1950), *aff'd per curiam*, 341 U.S. 918 (1951).

58. I use the term "mechanism" to refer to the class of items that authorize a search. The most common example of such a mechanism is a search warrant; the warrant is the item which authorizes officials to conduct a search. Alternatively, a statute may also be a mechanism authorizing a search. Examples include Title III, *see supra* Part III.B, and the mandatory Clipper statute.

59. 427 U.S. 463 (1976).

60. *Id.* at 479.

61. *Id.* at 479-482.

62. *Id.* at 480 n.10.

63. *See* *United States v. Riley*, 906 F.2d 841, 844-45 (2d Cir. 1990); *see also* *United States v. Hayes*, 794 F.2d 1348, 1354 (9th Cir. 1986), *cert. denied* 479 U.S. 1086 (1987) (search warrant upheld under similar circumstances).

64. *See* *In re Grand Jury Subpoena*, 920 F.2d 235, 239-40 (4th Cir. 1990).

65. *See* *United States v. Martin*, 866 F.2d 972, 977-78 (8th Cir. 1989).

66. *See* *United States v. Shoffner*, 826 F.2d 619, 630-32 (7th Cir.), *cert. denied*, 484 U.S. 958 (1987).

67. *See* *United States v. Wolfenbarger*, 696 F.2d 750, 752 (10th Cir. 1982).

68. 379 U.S. 476 (1965).

69. *Id.* at 477-79.

70. *Id.* at 485.

71. *See* *Lafayette Academy, Inc. v. United States*, 610 F.2d 1 (1st Cir. 1979).

72. *See* *United States v. Klein*, 565 F.2d 183, 186-87 (1st Cir. 1977).

73. *See* *United States v. McSurely*, 473 F.2d 1178, 1190 (D.C. Cir. 1972).

74. *Cf.* *Whiteley v. Warden, Wyoming State Penitentiary*, 401 U.S. 560, 564-66 (1971) (stating that the validity of a search warrant must be appraised by the facts revealed to the magistrate and not those later found to exist by executing officers); *United States v. Wuagneux*, 683 F.2d 1343, 1349 (11th Cir. 1982), *cert. denied*, 464 U.S. 814 (1983) ("It is universally recognized that the particularity requirement must be applied with a practical margin of flexibility, depending on the type of property to be seized, and that a description of property will be acceptable if it is as specific as the circumstances and nature of activity under investigation permit.")

75. *See* *Draper v. United States*, 358 U.S. 307, 313 (1959).

76. But compare the legislative history of Title III that envisions a judge issuing an electronic surveillance to consider probable cause that a crime "is being, has been, or *is about to be committed* by a particular person." S. REP. NO. 1097, 90th Cong. 2d Sess. 102 *reprinted in* 1968 U.S.C.C.A.N. 2191 (emphasis added). The Senate Report, citing *Berger*, states that this definition "is intended to reflect the test of the Constitution." *Id.* It appears to be erroneous to rely on *Berger* to justify the proposition that probable cause can be based on a crime that is about to be committed. The relevant excerpt of *Berger* states: "The purpose of the probable cause requirement of the Fourth Amendment, to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime

has been or is being committed" There is no mention of crimes that will be committed.

77. *See Katz*, 389 U.S. at 356-57.

78. *Berger*, 388 U.S. at 58-60.

79. The Particularity Clause applies only after the execution of a valid search warrant, founded upon "probable cause" and "supported by Oath or affirmation." U.S. CONST. amend. IV.

80. Mandatory Clipper thus also raises related First Amendment concerns because of its control on how citizens can converse with each other. *Cf.* John Markoff, *Federal Inquiry on Software Examines Privacy Programs*, N.Y. TIMES, Sept. 21, 1993, at D1 (quoting Eben Moglen, faculty member of Columbia Law School: "[t]he Government has no particular right to prevent you from speaking in a technological manner even if it is inconvenient for them to understand.")

81. *See supra* Part II.A.

82. *See, e.g.*, *United States v. Falon*, 959 F.2d 1143, 1148-49 (1st Cir. 1992) (annulling a warrant authorizing the seizure of books and computers because they were just as likely to be used for personal use as for criminal use); *United States v. Spilotro*, 800 F.2d 959, 967-68 (9th Cir. 1986) (disallowing a warrant because court could not sever particularized sections from the broad general language of the warrant).

83. Fourth Amendment scrutiny is tied to the expectations of the person being searched that his or her conduct will not be observed by the Government. The *Katz* court stated:

For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

Katz, 389 U.S. at 351-52 (citations omitted).

84. The permanent nature of mandatory Clipper alone, however, would likely not invalidate the scheme. When not activated, the Clipper chip is a dormant entity and is not part of any search. It is the combination of this permanent nature and its widespread use in an entire class of telephones that makes it an unprecedented means for the Federal Government to engage in surveillance.

85. In striking down the Clipper scheme, a court should not overly concern itself with the fear that its interpretation of the Particularity Clause applies Fourth Amendment doctrine too broadly. In *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965), Justice Douglas, writing for the Court about a constitutional right to privacy stated that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance."

Moreover, applying a section of the Fourth Amendment liberally to mandatory Clipper is not unprecedented even when considering a legitimate interest of the government to enforce laws effectively. The Supreme Court stated in *Gouled v. United States*, 255 U.S. 298, 304 (1921), that the Fourth Amendment "should receive a liberal construction, so as to prevent stealthy encroachment upon or 'gradual depreciation' of the rights secured by [it], by imperceptible practice of courts or by well-intentioned, but mistakenly over-zealous, executive officers."

86. *See also* *Mincey v. Arizona*, 437 U.S. 385, 393 (1978) ("[T]he mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment.")

87. Since law enforcement has come to rely heavily on electronic surveillance, the effect of Clipper's demise would be hard to predict. *See Fishman, supra* note 39, at 317 n.8.

88. *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting).

89. *See* Colin McEnroe, *Guide to High-tech Information Networks*, HARTFORD COURANT, Nov. 8, 1993, at A6. *Cf.* Melissa J. Perenson, *PC Execs Educate Congress on National Information Superhighway*, PC MAG., Nov. 23, 1993, at 32.

