

April 2002

Bits and Bytes: The Carnivore Initiative and the Search and Seizure of Electronic Mail

Sandy D. Hellums

Follow this and additional works at: <https://scholarship.law.wm.edu/wmborj>



Part of the [Constitutional Law Commons](#), and the [Fourth Amendment Commons](#)

Repository Citation

Sandy D. Hellums, *Bits and Bytes: The Carnivore Initiative and the Search and Seizure of Electronic Mail*, 10 Wm. & Mary Bill Rts. J. 827 (2002), <https://scholarship.law.wm.edu/wmborj/vol10/iss3/8>

BITS AND BYTES: THE CARNIVORE INITIATIVE AND THE SEARCH AND SEIZURE OF ELECTRONIC MAIL

This Note examines the application of Fourth Amendment search and seizure doctrines to the interception of electronic mail within the context of the FBI Carnivore initiative. The author argues that the traditional law of electronic surveillance's understanding of communication is outdated and never contemplated new technologies like Carnivore and their far reaching implications. Consequently, the author argues, that to protect our long-understood expectations of privacy, the search and seizure of electronic documents should be analyzed under the traditional papers analysis. To do so, the Supreme Court would afford the interception electronic documents the highest form of constitutional protect available under law.

The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways 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.¹

I. INTRODUCTION

Evolving communications technologies pose a challenge to civil libertarians and law enforcement. In particular, the privacy of electronic mail presents the unique challenge of requiring a new legal paradigm by which to analyze public policies seeking to balance the interests between individual rights and crime fighting. This Note examines the application of Fourth Amendment search and seizure doctrines to electronic mail within the context of the FBI Carnivore initiative. Two modes of legal analysis present themselves as possible standards for interception of e-mail: (1) those established for interception of traditional mail; or (2) those established for electronic surveillance. E-mail constitutes a hybrid means of communication combining the form of traditional papers with the manner of telephone conversations. Because of its unique nature, e-mail does not fit neatly within either paradigm. Currently, however, courts approach computer-based communications from the position of traditional electronic surveillance, subjecting it to those protections. This Note argues that search and seizure of electronic documents is better analyzed under a traditional papers analysis, affording it the highest form of constitutional protection. In addition, this Note applies both standards to the Carnivore initiative and analyzes the constitutionality of law enforcement interception of electronic mail addresses.

¹ Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

II. BACKGROUND: THE CARNIVORE INITIATIVE

The FBI electronic surveillance program known as Carnivore first came to light during an April 6, 2000 congressional Constitution subcommittee hearing.² There the Bureau revealed that it had utilized a new interception device approximately twenty-five times in the last two years.³

The project originated from a still-classified surveillance system deemed technologically deficient.⁴ In February 1997, it evolved into an FBI project known as Omnivore.⁵ The Omnivore system originally ran on a Solaris X86 computer and was replaced by the Windows NT-based computer in June 1999, which became known as Carnivore.⁶

According to the FBI, Carnivore is a special-purpose electronic surveillance system that allows for full communication content interceptions and pen register, as well as trap and trace investigations, to acquire addressing information.⁷ It is part of a group of software applications known as the "DragonWare suite" that allows law enforcement to capture, store, and process packets of electronic information.⁸ According to the FBI, the process works as follows:

Carnivore's filtering operates in stages. Carnivore's first action is to filter a portion of an ISP's highspeed [sic] network traffic. Specifically, it filters binary code - streams of 0's and 1's that flow through an ISP

² *ACLU Urges Congress to Put a Leash on "Carnivore" and Other Government Snoopware Programs*, ACLU Press Release (July 12, 2000), at <http://www.aclu.org/news/2000/n071200b.html>.

³ *Carnivore Diagnostic Tool: Hearings Before the Subcomm. on the Courts of the Senate Comm. on the Judiciary*, 106th Cong. (Sept. 6, 2000) (statement of Donald M. Kerr, Assistant Director Laboratory Division FBI) [hereinafter Kerr].

⁴ Kevin Poulsen, *Carnivore Details Emerge*, SECURITY FOCUS NEWS (Oct. 4, 2000), at <http://www.securityfocus.com/news/97> [hereinafter Poulsen].

⁵ *Id.*

⁶ Press Release, Electronic Privacy Information Center, *FBI Releases Carnivore Documents to EPIC* (Oct. 2, 2000), at http://www.epic.org/privacy/carnivore/foia_pr.html.

⁷ Kerr, *supra* note 3, at 6.

⁸ Poulsen, *supra* note 4. DragonWare is not the only available sniffer software. Several public software products enable interception of computer information packets. One of these, EtherPeek, enables a user to survey web usage as well as e-mail traffic. In a demonstration by the Illinois Institute of Technology Research Institute and Chicago-Kent College of Law, researchers found "the full content of the e-mail thus retrieved and the full content of the URLs and selected pages were clearly visible in the plain text ASCII window of the software." Thomas Gregory Motta, *Government and Electronic Privacy: Trends in Law Enforcement, Investigatory Tools and Protection of National Security*, in SECOND ANNUAL INSTITUTE ON PRIVACY LAW: STRATEGIES FOR LEGAL COMPLIANCE IN A HIGH-TECH AND CHANGING REGULATORY ENVIRONMENT 705 (Francoise Gilbert et al. eds. 2001) [hereinafter Motta].

network If the subject's identifying information is detected, the packets of the subject's communication associated with the identifying information that was detected, and those alone, are segregated for additional filtering or storage After exclusively segregating the subject's information for further machine processing, then a second stage of filtering is employed . . . Carnivore checks its programming to see what it should filter and collect for processing.⁹

The system operates at the ISP level and sniffs through literally millions of bits per second searching for the specific code associated with a criminal subject.¹⁰ It can be configured to gather only pen register, trap and trace transactional and addressing information, or comprehensively collect the entire message.¹¹

Under a pen register or trap and trace order, law enforcement is authorized to collect source, destination, date, time, duration, and user account address information.¹² Pen registers have been utilized for telephone surveillance and are recognized as constitutional by the Supreme Court.¹³ Traditionally, a pen register records "telephone numbers that are dialed from a phone, and trap and trace devices are used to determine the number of origin of a telephone call."¹⁴

Privacy advocates argue that traditional pen registers and trap and trace are much less intrusive than use of this new technique in cyberspace.¹⁵ Online, the contents of the messages and the sender information cannot be separated.¹⁶ With traditional telephone messages, information concerning the number called is sent prior to any message being created, but the conversation has not yet taken place. In contrast, an e-mail message contains the content of the message alongside the address to or from which it is being sent.

In addition, labeling information could include subject lines. A great deal of

⁹ Kerr, *supra* note 3, at 9.

¹⁰ *Id.*

¹¹ *Id.* at 9-10.

¹² *Id.* at 10.

¹³ See *Smith v. Maryland*, 442 U.S. 735 (1975).

¹⁴ *The Fourth Amendment and the Internet: Testimony Before the Subcomm. On the Constitution of the House Comm. on the Judiciary*, 106th Cong. (2000) (Apr. 6, 2000) (statement of Robert Corn-Revere, Partner, Hogan & Hartson L.L.P.), at <http://www.house.gov/judiciary/corn0406.htm>.

¹⁵ Privacy advocates active in electronic liberties include the American Civil Liberties Union (ACLU), Electronic Freedom Foundation (EFF), Electronic Privacy Information Center (EPIC), and Center for Democracy and Technology (CDT). See Motta, *supra* note 8, at 653. For a website critical of the initiative, see <http://www.stopcarnivore.com>.

¹⁶ *The Fourth Amendment and Carnivore: Statement of the Electronic Frontier Foundation Before the Subcomm. on the Constitution of the House Comm. On the Judiciary*, 106th Cong. (July 28, 2000), at http://www.eff.org/Privacy/Surveillance?Carnivore/20000728_eff_house_carnivore.html.

specific information may be intercepted and reviewed if the packet contains a subject line. The FBI contends that it limits such searches to transactional records as defined under the Electronic Communications Privacy Act of 1986.¹⁷ Such records include "addressing, routing, billing, or other information maintained or generated by the service provider . . . [but] do not include the content."¹⁸ Whether or not the system gathers actual content is highly debated, and the answer may only come with the further release of technical documentation by the FBI.

In addition, Carnivore may be used to obtain full communications of a particular criminal subject under an authorized Title III intercept.¹⁹ Configured for a full content collection, the software obtains information far beyond electronic mail.²⁰ Independent analysis conducted by the Illinois Institute of Technology in conjunction with the Chicago-Kent School of Law verified that Carnivore can "collect the contents of a target's e-mail."²¹ In addition, the software possesses a full collection mode that allows interception of all communications from a fixed IP address.²² Under this mode the system collects "web browsing contents, FTP login session, commands and data, and e-mail contents."²³

Proponents contend that the Carnivore initiative is an important tool in combating criminals of all ilks. "Now that most transactions and exchanges have become electronic, you really don't need to be an expert to predict that this will become, or already is, a crime generator."²⁴ The FBI argues that terrorists, spies, hackers, and other criminals are increasingly utilizing computer networks and electronic communications to develop and execute their plans.²⁵ As in prior privacy-versus-law enforcement debates, the Bureau points to several high profile cases to illustrate its point.²⁶ For example, terrorists such as Osama bin Laden and

¹⁷ Kerr, *supra* note 3, at 4-5.

¹⁸ *Id.* at 4.

¹⁹ *Id.* at 13.

²⁰ See Motta, *supra* note 8, at 684-85.

²¹ *Id.* at 685.

²² *Id.*

²³ *Id.*

²⁴ Thomas J. Talleur, *The Eavesdropping Society: Electronic Surveillance and Information Brokering*, in SECOND ANNUAL INSTITUTE ON PRIVACY LAW: STRATEGIES FOR LEGAL COMPLIANCE IN A HIGH-TECH AND CHANGING REGULATORY ENVIRONMENT 573 (Francoise Gilbert et al. eds., 2001) (quoting Lofk Weerd, Police Inspector and Computer Crime-Unit Expert, Haaglanden Regional Police, The Netherlands).

²⁵ See Kerr, *supra* note 3, at 1-3.

²⁶ Many of the same arguments and concerns have been expressed by law enforcement and privacy advocates in debates over digital telephony and encryption. For a complete discussion on these two issues, see WHITFIELD DIFFIE AND SUSAN LANDAU, *PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION* (1998); *THE ELECTRONIC PRIVACY PAPERS: DOCUMENTS ON THE BATTLE FOR PRIVACY IN THE AGE OF SURVEILLANCE* (Bruce Schneier & David Banisar eds., 1997) [hereinafter *THE ELECTRONIC PRIVACY PAPERS*].

Ramzi Yousef are utilizing computers to mastermind major attacks against the United States, and West German hackers have gained access to Department of Defense systems with the financial backing of the KGB.²⁷ Finally, the Bureau points to statistics illustrating the increasing use of the Internet for both financial fraud and child pornography.²⁸

Because of these new threats, it is argued, law enforcement must respond with ever-increasing forms of surveillance.²⁹ Communications interception plays an essential part in solving and preventing many crimes. From 1985 to 1991, court-ordered electronic surveillance conducted by the FBI led to 7,324 convictions, almost \$300 million in fines being levied, over \$750 million in recoveries, restitution and court ordered forfeitures, and close to \$2 billion in prevented potential economic loss.³⁰ The Carnivore initiative is only one in a series of attempts by law enforcement and Congress to combat this new form of crime.³¹

These new surveillance systems have been subject to the traditional legal standard created for wiretapping. Currently, all forms of electronic surveillance are subject to control under the Electronic Communications Privacy Act (ECPA), which amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).³²

Officers must obtain either a full Title III court order requiring probable cause for intercepting communications' content or an ECPA order based upon relevancy for communications' addressing and transactional record information.³³ To obtain a full content order, the application must particularly and specifically state the offense, the facility through which the communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted.³⁴

In addition, applications under Title III require the authorization of a high-level Department of Justice official and are subject to approval and review by federal district court judges.³⁵ Furthermore, applicants must indicate that other normal investigative techniques have failed, will not work, or are too dangerous.³⁶

²⁷ See generally STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION (1984).

²⁸ See Kerr, *supra* note 3, at 3-4.

²⁹ *Id.* at 16.

³⁰ *Testimony Before the Subcomm. On Technology, Environment and Aviation of the House Comm. on Science, Space and Technology*, 103d CONG. (1994) (statement of Dorothy Denning, Professor of Computer Science, Georgetown University).

³¹ See generally THE ELECTRONIC PRIVACY PAPERS, *supra* note 26.

³² 18 U.S.C. §§ 2510-2522 (2001).

³³ *Id.*

³⁴ *Id.*

³⁵ Kerr, *supra* note 3, at 13.

³⁶ *Id.*

Surveillance orders are also limited in duration and require periodic reporting to the courts.³⁷

It is unclear whether these traditional statutory concepts translate to the online environment. Unlike telephone taps, where the target's lines are accessed directly, electronic surveillance requires that a suspect's communications be picked out of millions of other documents being sent through cyberspace. This necessarily means searching through the private communications of non-suspects. As a matter of legal interpretation and practical application, existing statutes do not clearly apply to Internet communications.³⁸

In the online world, pen registers and trap and traces convey much more information than that of traditional phone communications. Furthermore, documents in electronic form may be better protected under traditional Fourth Amendment jurisprudence than under the law of electronic surveillance.

III. LAW OF TRADITIONAL MAIL

The Fourth Amendment explicitly recognizes an individual privacy interest in personal papers.³⁹ The Framers meant to protect it when drafting the Bill of Rights, and the courts have long held that a man's correspondence is held to the highest level of protection, as if it were an extension of the home.⁴⁰ The Fourth Amendment provides the most expansive protection against searches and seizures and most clearly delineates a right to be "left alone." Specifically, the amendment protects:

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.⁴¹

Unlike the privacy of persons and relationships that are found in numerous "penumbras" of the Bill of Rights, privacy of place and papers is fairly well outlined within the actual text of the Fourth Amendment.⁴² However, even it has had to evolve over time to clarify what places are protected from intrusion and what

³⁷ *Id.*

³⁸ See Corn-Revere, *supra* note 14, at <http://www.house.gov/judiciary/corn0406.htm>.

³⁹ U.S. CONST. amend. IV.

⁴⁰ See *Olmstead v. United States*, 277 U.S. 438, 457 (1928).

⁴¹ U.S. CONST. amend. IV.

⁴² See *Roe v. Wade*, 410 U.S. 113 (1973) (discussing privacy rights found within constitutional penumbras); *Griswold v. Connecticut*, 381 U.S. 479 (1965) (same).

the consequences are for the state when it violates individuals' rights.

The Court first recognized a right to privacy inherent within the Fourth Amendment in *Boyd v. United States*.⁴³ The case involved a seizure and forfeiture of thirty-five cases of plate glass thought to be in violation of customs laws.⁴⁴ The government ordered Boyd to produce invoices for the cases of glass.⁴⁵ The defendant argued that in a suit for forfeiture, no evidence can be compelled from the claimants themselves, and to compel production of evidence to be used against them is unconstitutional.⁴⁶

The Supreme Court agreed. Looking to English common law, Justice Bradley quoted Lord Camden as saying:

[E]very invasion of private property, be it ever so minute, is a trespass . . . papers are the owner's goods and chattels; they are his dearest property It is not the breaking of his doors, and rummaging of his drawers that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property.⁴⁷

In *Boyd*, the Court held that Fourth Amendment rights must be construed broadly to protect the essence of the search and seizure language.⁴⁸ "Constitutional provisions for the security of person and property should be liberally construed. A close and literal construction deprives them of half their efficacy, and leads to gradual deprecation of the right, as if it consisted more in sound than in substance."⁴⁹ Thus the Court laid the foundation for an expanding protection of privacy rights under the Fourth Amendment.

The amendment itself only makes mention of persons, houses, papers, and effects, but the Court never restricted constitutionally permissible claims of privacy against official intrusions to a literal reading of the Fourth Amendment.⁵⁰ While the Court eventually placed some limitations on privacy expectations in open spaces, it found a propertied basis for privacy protection in homes, offices, hotel rooms, apartments, automobiles, and taxicabs.⁵¹ The most obvious of these is the home —

⁴³ 116 U.S. 616 (1886).

⁴⁴ *Id.* at 618.

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.* at 627-28, 630.

⁴⁸ *Id.*

⁴⁹ *Id.* at 635.

⁵⁰ DAVID O'BRIEN, *PRIVACY, LAW AND PUBLIC POLICY* (1979).

⁵¹ *Id.* See e.g., *Stoner v. California*, 376 U.S. 483 (1964) (extending protection to hotel rooms); *Rios v. United States*, 364 U.S. 253 (1960) (extending protection to taxicabs); *Henry v. United States*, 361 U.S. 98 (1959) (extending protection to autos); *United States v. Jeffers*,

after all, "a man's home is his castle."

In particular, two cases exemplify the Court's protection of homes. *Weeks v. United States* involved a defendant who was charged with using the mail for the purpose of transporting items related to a lottery.⁵² Weeks was arrested by a police officer at his office without a warrant.⁵³ Other officers went to his house, where they located a key and entered.⁵⁴ A search of his room revealed numerous papers and other articles that officers turned over to a U.S. Marshal.⁵⁵ Later the same day, several other policemen returned with the same marshal and gained entry to the home by permission of a renter living there.⁵⁶ A second search revealed more documents.⁵⁷ Neither search was conducted pursuant to a search warrant and Weeks was subsequently convicted and sent to prison.⁵⁸ The Court held that the taking of documents without a warrant violated the constitutional rights of the defendant.⁵⁹

The Court's holding supported the *Boyd* decision finding that an individual's home and papers enjoy the utmost protection under the Fourth Amendment.⁶⁰ Justice Day wrote that the amendment:

[T]ook its origin in the determination of the framers of the Amendments to the Federal Constitution to provide for that instrument a Bill of Rights, securing to the American people, among other things, those safeguards which had grown up in England to protect the people from unreasonable searches and seizures, such as were permitted under the general warrants issued under authority of the Government by which there had been invasions of the home and privacy of the citizens and the seizure of their private papers in support of charges, real or imaginary, made against them.⁶¹

Weeks created the exclusionary rule prohibiting admission in federal courts of illegally seized evidence.⁶² Day argued that to allow the introduction of illegally

342 U.S. 48 (1951); *Lustig v. United States*, 338 U.S. 74 (1949); *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920) (extending protection to offices).

⁵² 232 U.S. 383 (1914).

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ *Id.*

⁵⁸ *Weeks*, 232 U.S. at 383.

⁵⁹ *Id.*

⁶⁰ *Id.*

⁶¹ *Id.* at 390.

⁶² *Id.*

seized materials would be to "affirm by judicial decision a manifest neglect, if not an open defiance, of the constitution."⁶³ The Fourth Amendment safeguards individuals from unreasonable searches and seizures, and therefore requires the exclusion at trial of any evidence unlawfully obtained.⁶⁴

The exclusionary rule, however, did not immediately apply to the states. In fact, the Supreme Court directly rejected its application to the states under the Fourteenth Amendment in *Wolf v. Colorado*.⁶⁵ Not until the 1961 case of *Mapp v. Ohio* did the exclusionary rule apply to evidence offered in a criminal trial in a state court.⁶⁶

A right had finally found a remedy. In *Weeks*, Day agreed with Cooley's earlier assessment when he quoted: "[T]he maxim that 'every man's house is his castle' was made a part of our constitutional law in the clauses prohibiting unreasonable searches and seizures, and has always been looked upon as of high value to the citizen."⁶⁷ Papers are a fundamental component of the Fourth Amendment and, as such, receive the highest degree of protection — equal to that of homes. The equating of the privacy afforded to mail to the privacy afforded to the home is due in large part to the fact that letters are sealed. The same cannot be said for non-encrypted electronic mail.⁶⁸ For current analysis, this area of the law may be divided into two subsections: full content interceptions of mail and mail covers.

A. Full Content Interceptions

The standard for protection of traditional mail turns on whether it is a first class parcel or otherwise closed for inspection or sought to be sent in the most expeditious class of mail.⁶⁹ There are a number of cases that have developed the standard by which traditional mail may be searched and seized.

The Court first dealt with mail searches in *Ex Parte Jackson*.⁷⁰ In *Jackson*, the Court granted the fullest protection to mail, stating that:

Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and

⁶³ *Id.* at 394.

⁶⁴ See generally O'BRIEN, *supra* note 50.

⁶⁵ 338 U.S. 25 (1949).

⁶⁶ 367 U.S. 643 (1961).

⁶⁷ *Weeks*, 232 U.S. at 390.

⁶⁸ For a discussion of encryption and its impact on the law of electronic surveillance, see Megan Connor Bertron, *Home is Where Your Modem Is: An Appropriate Application of Search and Seizure Law to Electronic Mail*, 34 AM. CRIM. L. REV. 163, 192 (1996).

⁶⁹ WAYNE LAFAYE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT (3d ed. 1996).

⁷⁰ 96 U.S. 727 (1878).

weight, as if they were retained by the parties forwarding them in their own domiciles. . . . Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subject to search in one's own household.⁷¹

Searches of letters deposited in the mail are governed by the warrant requirements of the Fourth Amendment. A person sending a sealed envelope via First Class U.S. Mail has a reasonable expectation of privacy in the contents.⁷² Contrast *Ex Parte Jackson* with *United States v. Van Leeuwen*,⁷³ where the method of shipment played an important role in the Court finding that an unwarranted detention did not violate the Fourth Amendment. The defendant shipped two packages via "airmail registered" mail from Washington to two separate locations.⁷⁴ The postal clerk noticed that the return address was actually a vacant home and consequently notified police.⁷⁵ The packages were thus detained for twenty-nine hours in order for the police to investigate the destination of the two packages.⁷⁶ The investigation revealed that both addressees were currently suspected of drug trafficking.⁷⁷ This information formed the basis of a search warrant that then allowed officers to open and inspect the packages, after which they were forwarded.⁷⁸ The Court held that such a detention did not violate the Fourth Amendment:

No interest protected by the Fourth Amendment was invaded by forwarding the packages the following day rather than the day when they were deposited. The significant Fourth Amendment interest was in the privacy of this first-class mail; and that privacy was not disturbed or invaded until the approval of the magistrate was obtained.⁷⁹

The Court did not go so far as to say that any detention of mail is allowed; rather, it noted that the facts of the case and the general suspicious nature of the packages made a one-day delay reasonable under the Fourth Amendment.⁸⁰ The expectation of how fast a package should arrive at its destination thus affects the

⁷¹ *Id.* at 733.

⁷² *United States v. Van Leeuwen*, 397 U.S. 249 (1970).

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ *Id.*

⁷⁶ *Id.*

⁷⁷ *Id.*

⁷⁸ *Van Leeuwen*, 397 U.S. at 249.

⁷⁹ *Id.* at 253.

⁸⁰ *Id.*

level of protection provided to its detention.

However, statutory protections provide that mail may not be opened except under authority of a search warrant authorized by law.⁸¹ Although it may be detained without a warrant, the actual searching of a first class package's contents requires judicial approval.⁸²

No letter of such a class⁸³ of domestic origin shall be opened except under authority of a search warrant authorized by law, or by an officer or employee of the Postal Service for the sole purpose of determining an address at which the letter can be delivered, or pursuant to the authorization of the addressee.⁸⁴

Thus, the same constitutional protections afforded to the searching of papers within the home, subject to search warrant, are given to first-class mail.⁸⁵

B. Mail Covers

In contrast to full content searches, mail covers have long been allowed to obtain information from the exterior of a parcel. Postal regulations first authorized mail covers in 1893,⁸⁶ but their widespread use did not come to light until the McCarthy investigation of 1952.⁸⁷ Law enforcement may nonconsensually record any information on the outside of a sealed mail item or record the contents of an unsealed mail matter.⁸⁸ This information may be obtained for five purposes: (1) to protect national security; (2) locate a fugitive; (3) obtain evidence of commission or attempted commission of a crime; (4) obtain evidence of a violation or attempted

⁸¹ 39 U.S.C. § 3623(d) (2001).

⁸² 39 U.S.C. § 3623 (2001).

⁸³ This refers to the class of mail providing the most expeditious handling and transportation. *See* 39 U.S.C. § 3623(d) (2001).

⁸⁴ *Id.*

⁸⁵ *United States v. Fulcher*, 229 F. Supp. 456 (1964). As the options and speeds available for mailing parcels increases, what constitutes the most expeditious means of handling mail becomes less clear. In general, "classification of mails is based not upon merely inherent distinctions or differences in nature and character of articles as mailable matter and cost of their carriage, but also rests upon broad principles of public policy." 39 U.S.C. § 3623 (Interpretive Notes and Decisions) (quoting *Lewis Publ'g Co. v. Morgan*, 229 U.S. 288, 303 (1913)).

⁸⁶ Daniel E. Feld, Annotation, *Validity, Under Fourth Amendment, of "Mail Cover"*, 57 A.L.R. FED. 742, 743 (1999).

⁸⁷ *Invasion of Privacy: Use and Abuse of Mail Covers*, 4 COLUM. J.L. & SOC. PROBS. 165 (1968).

⁸⁸ 39 C.F.R. § 233.3 (2001); *see* JOHN WESLEY HALL, *SEARCH AND SEIZURE* (3d ed. 2000).

violation of a postal statute; or (5) assist in the identification of forfeitable property.⁸⁹

The chief postal inspector possesses the authority to grant such a search, although this power may be granted to others except in instances implicating national security.⁹⁰ A mail cover order may be issued under the following situations:

1. When a written request is received from a postal inspector that states reason to believe a mail cover will produce evidence relating to the violation of a postal statute.
2. When a written request is received from any law enforcement agency in which the requesting authority specifies the reasonable grounds to demonstrate the mail cover is necessary to [fulfill one of five objectives discussed *supra* note 89 and accompanying text.]
3. When time is of the essence, the Chief Postal Inspector, or designee, may act upon an oral request to be confirmed by the requesting authority in writing within three calendar days.⁹¹

The statute, therefore, grants the power to search on reasonable grounds and without approval of an outside, detached magistrate.⁹² This contrasts with the warrant requirement of full content searches and grants a lesser degree of protection to the information contained on the outside of a package. The courts have found this does not constitute a violation of the Fourth Amendment:

[A] mail cover does not violate plaintiff's Fourth Amendment rights where cover does not include examination of contents of mail, and persons who sent or received mail know or ought to know that postal employees must examine outside of mail in order to deliver it and, even if plaintiffs harbor subjective expectation of privacy, expectation is unreasonable in that persons who send mail to plaintiffs voluntarily expose information on outside of envelopes to postal employees.⁹³

Thus, the constitutionality of mail covers rests on the diminished expectation of privacy individuals have in the information contained on the outsides of packages. The Supreme Court upheld the constitutionality of these searches in *United States*

⁸⁹ 39 C.F.R. § 233.3 (2001).

⁹⁰ 39 C.F.R. § 233.3(d) (2001).

⁹¹ 39 C.F.R. § 233.3(e) (2001).

⁹² *Id.*

⁹³ Feld, *supra* note 86, at 20 (quoting *Vreeken v. Davis*, 718 F.2d 343 (1983)).

v. Jacobsen.⁹⁴ In *Jacobsen*, the Court held that the Fourth Amendment did not require the DEA to obtain a search warrant before testing a substance leaking from a package.⁹⁵ It reasoned that "it is constitutionally reasonable for law enforcement officials to seize 'effects' that cannot support a justifiable expectation of privacy without a warrant based on probable cause to believe they contain contraband."⁹⁶

IV. LAW OF ELECTRONIC SURVEILLANCE

Courts approach the protection of electronic communications from illegal search and seizure differently than of traditional correspondence. Although the courts have not accorded electronic speech the same level of deference as traditional speech, it is within the context of wiretapping that the Supreme Court articulated that the right to privacy belongs to people and not places.⁹⁷ In addition, searches of electronic communications are governed by statutory requirements.⁹⁸

A. Full Content Interceptions — Constitutional Requirements

Prior to the *Olmstead v. United States* decision in 1928, the Court built privacy upon a conception of physical space.⁹⁹ As new technologies developed, the Court began to consider invasions of another sort. Wiretapping, eavesdropping, and other electronic monitoring devices became increasingly common in police investigations during the early 1900s. As a consequence, the right of privacy had to be reconsidered in light of searches without a trespass and seizures without physical evidence.¹⁰⁰ The Court began to address the privacy of communications in *Olmstead*.¹⁰¹

Olmstead was convicted in the district court for the Western District of Washington for conspiracy to violate the National Prohibition Act for unlawfully possessing, transporting, and importing intoxicating liquors and maintaining nuisances, and selling intoxicating liquors.¹⁰² The information that led to the discovery of the conspiracy and its nature and extent was obtained through intercepting messages on the telephones of the conspirators by federal prohibition

⁹⁴ 466 U.S. 109 (1983).

⁹⁵ *Id.*

⁹⁶ *Id.* at 112-22. See also *United States v. Choate*, 576 F.2d 165 (9th Cir. 1978); *United States v. Costell*, 255 F.2d 876 (2d Cir. 1958); *Oliver v. United States*, 239 F.2d 818 (8th Cir. 1957).

⁹⁷ See *Katz v. United States*, 389 U.S. 347 (1967).

⁹⁸ 18 U.S.C. §§ 2510-2522 (2001).

⁹⁹ See *Boyd v. United States*, 16 U.S. 616 (1886).

¹⁰⁰ *Id.*

¹⁰¹ 277 U.S. 438 (1928).

¹⁰² *Id.*

officers.¹⁰³ Small wires were inserted along the ordinary telephone wires from the residences of four of the conspirators as well as those leading from the main office.¹⁰⁴ The insertions were made without trespass upon any property of the defendants;¹⁰⁵ the office taps were made in the basement of a large office building, and¹⁰⁶ the home taps were made in the streets near the house.¹⁰⁷

The Court utilized the property-based claims that underlie the *Boyd* decision.¹⁰⁸ The Court construed privacy protection as resting on the maxim of "a man's home is his castle":

Legitimate claims to the privacy of individuals' engagements arose with regard to and were justifiable in terms of the locus of the individuals' engagements as defined by proprietary interests. Privacy claims were strongest in so-called "constitutionally protected areas", particularly in one's house, and were enforced by the express requirements of the Fourth Amendment as well as the judicially constructed mere evidence and exclusionary rules.¹⁰⁹

In the case of *Olmstead*, there were no constitutionally protected areas.¹¹⁰ The Court strictly construed the Fourth Amendment to apply only to material things — the person, the house, his papers, or his effects.¹¹¹ However, this protection did not apply to private communications.¹¹² Justice Taft wrote:

The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants. By the invention of the telephone 50 years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place. The language of the Amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his

¹⁰³ *Id.*

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

¹⁰⁷ *Olmstead v. United States*, 277 U.S. 438 (1928).

¹⁰⁸ *Boyd v. United States*, 116 U.S. 616, 630-38 (1886).

¹⁰⁹ O'BRIEN, *supra* note 50, at 50.

¹¹⁰ *Olmstead*, 277 U.S. at 464.

¹¹¹ *Id.*

¹¹² *Id.*

house or office, any more than are the highways along with they are stretched.¹¹³

To expand the Fourth Amendment's application to communications, as Olmstead argued, would unduly enlarge the Amendment.¹¹⁴ It would apply search and seizure protection to the mere act of hearing or seeing the conversation of another.¹¹⁵ In the Court's view, it would be an unusual understanding to apply to the Fourth Amendment.¹¹⁶ The majority held that a person who utilizes telephone equipment intends for his/her voice to be projected out into the world, therefore there was no reasonable expectation of privacy.¹¹⁷

Justice Brandeis, in a most prophetic dissent, rejected the literal, property-based conception of privacy that the majority attributed to *Boyd*.¹¹⁸ He argued that the narrow language of the Amendment had been construed in a broader sense.¹¹⁹ He wrote: "[T]he makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . . They conferred, as against the Government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men."¹²⁰

Because people had this broad-based individual privacy, wiretapping surely violated it.¹²¹ Looking to *Ex parte Jackson*,¹²² Brandeis wrote: "[T]he evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails."¹²³ Furthermore, he wrote:

"[T]ime works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.¹²⁴

Brandeis's foresight would prove impeccable. However, the Court would not

¹¹³ *Id.* at 464-65.

¹¹⁴ *Id.* at 464.

¹¹⁵ *Id.*

¹¹⁶ *Olmstead*, 277 U.S. at 464.

¹¹⁷ *Id.*

¹¹⁸ *Id.* (Brandeis, J., dissenting).

¹¹⁹ *Id.* (Brandeis, J., dissenting).

¹²⁰ *Id.* at 478. (Brandeis, J., dissenting).

¹²¹ *Id.* (Brandeis, J., dissenting).

¹²² *Ex parte Jackson*, 96 U.S. 727 (1878).

¹²³ *Olmstead*, 277 U.S. at 475.

¹²⁴ *Id.* at 473. (citations omitted).

heed his words until 1967.¹²⁵ Until the Court decided *Katz v. United States*,¹²⁶ they stuck primarily with the *Boyd-Olmstead* construction of the Fourth Amendment — basing the right to privacy upon a property interest.¹²⁷

Following *Olmstead*, Congress passed the Federal Communications Act of 1934. Section 605 of the Act provides that no person who, as an employee, has to do with the sending or receiving of any interstate communication by wire shall divulge or publish it or its substance to anyone other than the addressee or his authorized representative or to authorized fellow employees, save:

[I]n response to a subpoena issued by a court of competent jurisdiction or on demand of other lawful authority. 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.¹²⁸

The Court utilized this Act to largely avoid the issue of electronic surveillance as a Fourth Amendment privacy issue. Instead, they viewed issues of wiretapping as dealing with interpreting and applying Section 605.¹²⁹ In *Nardone v. United States*, the Court utilized this tactic, finding that Section 605 precluded federal officers from wrongfully obtaining evidence through intercepted telephone messages.¹³⁰

In *Goldman v. United States*, the Court returned to the *Olmstead* theory, ruling that conversations overheard with a dictaphone were admissible.¹³¹ A dictaphone is a listening apparatus that could be placed up against a wall to overhear conversations in the next room.¹³² They found that use of the device did not constitute an illegal trespass or unlawful entry, and therefore did not violate the Fourth Amendment.¹³³ In contrast, however, they found that a dictaphone, a device requiring placement within the walls, was a violation because it required entrance into the defendant's home for installation.¹³⁴

¹²⁵ *Katz v. United States*, 389 U.S. 347 (1967).

¹²⁶ *Id.*

¹²⁷ See, e.g., *On Lee v. United States*, 343 U.S. 747 (1952); *Goldman v. United States*, 316 U.S. 129 (1942); *Hester v. United States*, 265 U.S. 57 (1924); *Perlman v. United States*, 247 U.S. 7 (1918) (relying on trespass theory to uphold searches).

¹²⁸ 47 U.S.C. § 605(a) (2001).

¹²⁹ O'BRIEN, *supra* note 50, at 54.

¹³⁰ *Nardone v. United States*, 308 U.S. 338 (1939).

¹³¹ *Goldman v. United States*, 316 U.S. 129 (1942).

¹³² *Id.*

¹³³ *Id.*

¹³⁴ *Id.*

The Court would continue to employ this logic in *Silverman v. United States*.¹³⁵ In *Silverman*, officers overheard conversations concerning gambling offenses by means of an electronic listening device that had been pushed through the party wall of an adjoining house until it touched the heating ducts in the house occupied by Silverman.¹³⁶ The Court held that the eavesdropping was accomplished by means of an unauthorized physical penetration into the premises, therefore violating their rights under the Fourth Amendment.¹³⁷ The Court stated: “[E]avesdropping accomplished by means of such a physical intrusion is beyond the pale of even those decision in which a closely divided Court has held that eavesdropping accomplished by other electronic means did not amount to an invasion of Fourth Amendment rights.”¹³⁸

They refused, however, to address the larger Fourth Amendment question presented by the case. The Court stated: “[T]he facts of the present case, however, do not require us to consider the large questions which have been argued. We need not here contemplate the Fourth Amendment implications of these and other frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society.”¹³⁹ This reexamination would take place six years later in *Katz v. United States*.¹⁴⁰

Katz was convicted in the district court for the Southern District of California for transmitting wagering information by telephone from Los Angeles to Miami and Boston.¹⁴¹ Evidence was admitted of telephone conversations overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from which Katz had placed his calls.¹⁴² The Court directly overturned *Olmstead*, stating:

We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the “trespass” doctrine there enunciated can no longer be regarded as controlling. The Government’s activities in electronically listening to and recording the petitioner’s words violated the privacy upon which he justifiably relied on while using the telephone booth and thus constituted a “search and seizure” within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to

¹³⁵ *Silverman v. United States*, 365 U.S. 505 (1961).

¹³⁶ *Id.*

¹³⁷ *Id.*

¹³⁸ *Id.* at 509-10.

¹³⁹ *Id.* at 509.

¹⁴⁰ 389 U.S. 347 (1967).

¹⁴¹ *Id.*

¹⁴² *Id.*

penetrate the wall of the booth can have no constitutional significance.¹⁴³

The Court held that the Fourth Amendment protects people, not places, and that individuals can make ideas and feelings very public from inside their homes as well as expect certain levels of privacy out in the world.¹⁴⁴ This is consistent with the Court's finding that individuals enjoy a certain amount of personal privacy when in hotels, others' apartments, or taxicabs, and so do their conversations.¹⁴⁵ The Fourth Amendment extends beyond these constitutionally protected areas to include oral statements, and therefore the physical intrusion standard established by *Olmstead* was rejected.

Under what conditions, then, could the government employ electronic surveillance? In *Katz*, the Court generally referred to a "strong probability" of wrongdoing that must be present and stated the surveillance be limited in scope and in duration to the specific purpose of establishing the contents of the petitioner's unlawful telephone communications.¹⁴⁶ More specifically, the Court stated, "under sufficiently 'precise and discriminate circumstances,' a federal court may empower government agents to employ a concealed electronic device for the narrow and particularized purpose of ascertaining the truth of the . . . allegations of a detailed factual affidavit alleging the commission of a specific criminal offense."¹⁴⁷

The Court clearly delineated the constitutional requirements underlying Fourth Amendment surveillance in *Berger v. New York*.¹⁴⁸ The case, decided a few months before *Katz*, struck down a New York Statute permitting eavesdropping.¹⁴⁹ They found the language of Section 813-a of the New York Code of Criminal Procedure was "too broad in its sweep resulting in a trespassory intrusion into a constitutionally protected area and is, therefore, violative of the Fourth and Fourteenth Amendments."¹⁵⁰ The Court detailed three standards for evaluating a justifiable "eavesdropping" search and seizure.¹⁵¹

First, the Fourth Amendment requires that a neutral and detached authority be interposed between the police and the public.¹⁵² Second, a warrant may only be issued upon probable cause, meaning the facts and circumstances within the affiant's knowledge and of which he has reasonably trustworthy information are sufficient unto themselves to warrant a man of reasonable caution to believe that an

¹⁴³ *Id.* at 353.

¹⁴⁴ *Id.*

¹⁴⁵ *See, e.g., supra* note 51.

¹⁴⁶ *Katz v. United States*, 389 U.S. 347, 354 (1967).

¹⁴⁷ *Id.* at 355. (citations omitted).

¹⁴⁸ *Berger v. New York*, 388 U.S. 41 (1967).

¹⁴⁹ *Id.*

¹⁵⁰ *Id.* at 44.

¹⁵¹ *Id.*

¹⁵² *Id.*

offense has been or is being committed.¹⁵³ Finally, the Fourth Amendment requires “particularly describing the place to be searched, and the persons or things to be seized.”¹⁵⁴ The Court in *Berger* held: “[T]he need for particularity and evidence of reliability in the showing required when judicial authorization of a search is sought is especially great in the case of eavesdropping. By its very nature eavesdropping involves an intrusion on privacy that is broad in scope.”¹⁵⁵

Since *Katz*, the technologies of eavesdropping have grown, as has the importance of information being transmitted. It is no wonder that there have been a number of attempts to protect legislatively individual privacy as well as law enforcement surveillance.

B. Full Content Interceptions — Statutory Requirements

Title III, as amended by the ECPA, serves as the primary statute protecting electronic communications. After the Court determined that electronic surveillance falls within the purview of the Fourth Amendment,¹⁵⁶ Congress codified the constitutional requirements in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.¹⁵⁷ In 1986, Congress further amended the Act to protect electronic communications, and thus re-titled it the Electronic Communications Privacy Act of 1986.¹⁵⁸ Most recently, Congress further amended the statute ostensibly to provide law enforcement easier access to digital communications technology by enacting the Communications Assistance for Law Enforcement Act (CALEA).¹⁵⁹

¹⁵³ *Id.* See also *Brinegar v. United States*, 338 U.S. 160 (1949); *Husty v. United States*, 282 U.S. 694 (1931); *Carroll v. United States*, 267 U.S. 132 (1925).

¹⁵⁴ *Berger v. New York*, 388 U.S. 41 (1967); see also *Silverman v. United States*, 365 U.S. 505 (1961).

¹⁵⁵ *Id.* at 56.

¹⁵⁶ See *Katz*, 389 U.S. 347 (1967); *Berger v. New York*, 388 U.S. 41 (1967).

¹⁵⁷ 18 U.S.C. §§ 2510-2520 (2001).

¹⁵⁸ 18 U.S.C. §§ 2510-2521 (2001).

¹⁵⁹ 18 U.S.C. § 2522 (2001) (enforcing CALEA, 47 U.S.C. § 1001, by expanding access to all forms of surveillance). CALEA requires telecommunications carriers to install wiretap facilities in all relay stations for police access. The law attempts to address the supposed difficulty of tracing cellular and some digital telephone conversations. It does not however, apply to computer information systems such as the Internet, Prodigy, or AOL. 47 U.S.C. § 1001.

CALEA instituted extensive regulations providing police agencies with facilitated wiretap capabilities. THE ELECTRONIC PRIVACY PAPERS, *supra* note 26, at 85-86. The statute purportedly balanced three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly power and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies. *Id.*

The statute's specific capability requirements are: (1) expeditiously isolate the content

ECPA protects wire,¹⁶⁰ oral,¹⁶¹ and electronic¹⁶² communications from illegal interceptions. In order for law enforcement to conduct an interception, numerous requirements must be met. First, a high level official must authorize application for a wiretap.¹⁶³ Second, wiretaps are restricted to investigation of felonies.¹⁶⁴ Third, an Article III judge must grant the order.¹⁶⁵ Fourth, probable cause must be demonstrated, and it must be shown that normal investigative procedures are

of a targeted communication within its service area; (2) isolate call identifying information about the origin and destination of a targeted communication; (3) enable the government to access isolated communications at a point away from the carrier's premises and on facilities procured by the government; and (4) do so unobtrusively and in such a way that protects the privacy and security of communications not authorized to be intercepted. 47 U.S.C. § 1001.

CALEA contains seven components designed to enhance personal privacy. THE ELECTRONIC PRIVACY PAPERS, *supra* note 26, at 80-82. First, it requires a court order rather than a subpoena to obtain e-mail address and other transactional data from electronic communications service providers. *Id.* Secondly, it expressly provides that the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information. *Id.* Third, it allows any person to petition the FCC for review of standards implementing wiretap capability requirements. *Id.* Fourth, it does not require mobile service providers to reconfigure their networks to deliver the content of communications occurring outside a carrier's service area. *Id.* CALEA also extends privacy protections of the ECPA to cordless phones and requires intervention of common carriers' personnel for switch-based interceptions, meaning law enforcement may not activate interceptions remotely or without the knowledge of a telecommunications carrier. Finally, it does not forbid the use of encryption technology. *Id.*

¹⁶⁰ 18 U.S.C. § 2510(1) defines wire communication as:

[A]ny aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication . . .

Id.

¹⁶¹ 18 U.S.C. § 2510(2) defines oral communication as: "[A]ny oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication."

¹⁶² 18 U.S.C. § 2510(12) defines electronic communication as: "[A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate commerce . . ."

¹⁶³ 18 U.S.C. § 2516(1) (2001).

¹⁶⁴ *Id.* at § 2516(3).

¹⁶⁵ *Id.* at § 2518(3).

insufficient.¹⁶⁶ Fifth, the order must specifically contain:

1. the identity of the interceptee; 2. the nature and location of the communications facilities to which the authority to intercept is granted;
3. a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;
4. the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and 5. the period of time during which such interception is authorized.¹⁶⁷

Sixth, the interception must be minimized to achieve the objective.¹⁶⁸ Seventh, after termination of the intercept the judge must notify those parties whose communications were intercepted.¹⁶⁹

These protections seem to guarantee, if not expand, the constitutional requirements for interception of communications. However, the ECPA provides differing treatment for oral/wire communications and electronic communications such as e-mail. There are three basic differences in the ECPA's treatment of electronic communications.¹⁷⁰ First, it may be intercepted for any felony rather than an enumerate list that limits oral and wire intercepts.¹⁷¹ Second, an electronic intercept does not need a court order, but may be authorized by an Attorney General.¹⁷² Finally, the exclusionary provision of the statute does not apply to electronic communications.¹⁷³ Thus, any information obtained by illegally intercepting electronic communications may still be utilized in prosecuting the individual. This is in stark contrast to the exclusionary protections provided traditional papers and essentially strips a right of any remedy.

C. Partial Content Interceptions — Trap & Trace and Pen Register Devices

Pen register and trap and trace devices provide law enforcement with numbers dialed from or to the line to which it is attached.¹⁷⁴ For example, law enforcement would attach a pen register to the phone of a suspect in order to obtain a list of numbers called. In contrast, a trap and trace device might be used on a victim's line

¹⁶⁶ *Id.* at § 2518(3).

¹⁶⁷ Motta, *supra* note 8, at 663.

¹⁶⁸ 18 U.S.C. § 2518(5) (2001).

¹⁶⁹ 18 U.S.C. § 2518(8) (2001).

¹⁷⁰ See Robert S. Steere, *Keeping 'Private E-Mail' Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U. L. REV. 231, 256 (1998).

¹⁷¹ *Id.*

¹⁷² *Id.*

¹⁷³ *Id.*

¹⁷⁴ *United States v. Giordano*, 416 U.S. 505, 549 (1974).

to determine a call's origin number.¹⁷⁵ Statutory criminal procedure allows a government attorney to apply for approval to utilize these techniques in an ongoing investigation.¹⁷⁶ An application must be made to a court of competent jurisdiction and include both the identity of the investigative officer making the application and a certification that the information to be obtained is relevant to an ongoing criminal investigation.¹⁷⁷ The statute contains no probable cause requirement for this type of search, and the Court has found that such investigations do not constitute a search requiring a warrant under the Fourth Amendment.¹⁷⁸

Smith involved a robbery victim receiving threatening phone calls from an individual identifying himself as the perpetrator.¹⁷⁹ Police, without obtaining a search warrant or court order, installed a pen register at the telephone company's main switching station to monitor phone numbers dialed by a suspect in the case.¹⁸⁰

In determining whether the Fourth Amendment had been violated, the Court asked whether the person invoking the protection could claim a justifiable, reasonable, or legitimate expectation of privacy that had been invaded by government.¹⁸¹ This inquiry involves two questions: (1) whether the individual has exhibited an actual subjective expectation of privacy; and (2) whether this subjective expectation is one society is prepared to recognize as reasonable.¹⁸²

The Court found no expectation of privacy in the numbers called.¹⁸³ Distinguishing the case from *Katz*, they pointed to the fact that pen registers do not acquire any contents of the communications.¹⁸⁴ Instead, the pen register only detects the means of establishing communication — the tones that connect one phone with another; as such, a person has no reasonable expectation of privacy in dialing information because people understand that these tones must be transmitted to another in order for the technology to work.¹⁸⁵ Information voluntarily turned over to third parties has consistently been held to contain no legitimate expectation

¹⁷⁵ 18 U.S.C. § 3127(3) defines pen register as: "[A] device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached . . ."; *Id.* Section 3127(4) defines a trap and trace device as: "[A] device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted . . ."

¹⁷⁶ *Id.* at § 3122(a).

¹⁷⁷ *Id.* at § 3122(b).

¹⁷⁸ See *Smith v. Maryland*, 442 U.S. 735 (1979).

¹⁷⁹ *Id.* at 737.

¹⁸⁰ *Id.* at 735.

¹⁸¹ *Id.* at 739 (quoting *Katz v. United States*, 389 U.S. 347 (1967)).

¹⁸² *Id.*

¹⁸³ *Id.*

¹⁸⁴ *Id.* at 741.

¹⁸⁵ *Id.*

of privacy.¹⁸⁶

The dissent argued that the numbers dialed are akin to the content protected under *Katz*. The Court reasoned that a person making calls from his home certainly would want to keep who they were calling private.¹⁸⁷

Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called . . . [to do so would] reveal the most intimate details of a person's life.¹⁸⁸

The dissenters in *Katz* also argued that allowing warrantless interceptions of pen registers ignores the vital role that telephone communications play in everyday life.¹⁸⁹ "To hold otherwise ignores the vital role telephonic communication plays in our personal and professional relationships."¹⁹⁰

In addition to finding that pen registers and trap and trace devices do not fall within the scope of the Fourth Amendment, the Court also held that protections provided to other interceptions under 18 U.S.C. § 2518 do not apply.¹⁹¹ The Court in *New York Telephone* distinguished Title III as not governing the authorization of the use of pen registers because they do not acquire the contents of communications:¹⁹²

[A] law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed — a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.¹⁹³

Because of the limited scope of the intercept, it does not qualify for the highest level of Fourth Amendment protection. Rather, the restrictions are quite limited, subject

¹⁸⁶ *Id.* at 743-44. *See, e.g.,* *United States v. Miller*, 425 U.S. 442 (1976); *Hoffa v. United States*, 385 U.S. 293 (1966); *Lopez v. United States*, 373 U.S. 427 (1963).

¹⁸⁷ *Smith v. Maryland*, 442 U.S. 735, 746 (1979) (Stewart, J., dissenting).

¹⁸⁸ *Id.* at 748.

¹⁸⁹ *Id.* at 751. (Marshall, J., dissenting).

¹⁹⁰ *Id.* (Marshall, J., dissenting).

¹⁹¹ *United States v. N. Y. Tel. Co.*, 434 U.S. 159 (1977).

¹⁹² *Id.* at 166.

¹⁹³ *Id.* at 167.

only to an ongoing investigation requirement.¹⁹⁴

V. INTERCEPTION OF ELECTRONIC MAIL

As a burgeoning means of communications, citizens continue to increase their reliance upon electronic mail usage. E-mail has widely replaced the telephone and traditional mail in business, educational, and personal settings. The Florida Supreme Court stated: "[E]-mail transmissions are quickly becoming a substitute for telephonic and printed communications, as well as a substitute for direct oral communications."¹⁹⁵ Under what level of protection the search and seizure of electronic mail falls is a question the courts have not answered:

Because email communications take the place of both oral *and* written communications, can be saved electronically (and therefore potentially accessed by systems operators), printed in hard copy, and easily re-transmitted by recipients, the privacy rights of senders and recipients of e-mail (at least in unencrypted form) are still being defined by courts.¹⁹⁶

The two possible treatments of e-mail are as electronic surveillance or traditional correspondence. Courts have chosen the former and protect electronic mail under the ECPA.¹⁹⁷ The ECPA requires either a warrant or subpoena for disclosure of the contents of electronic communications.¹⁹⁸ "The law applies most of the same prohibitions and requirements to the interception of electronic communications as it does to telephone (wire) communications."¹⁹⁹ The Act distinguishes between the interception of messages as they are sent and the searching of electronic storage.²⁰⁰ The Department of Justice has developed guidelines for the searching and seizing of computers that are distinguishable from the interception of electronic communications.²⁰¹

¹⁹⁴ See also William A. Claerhout, *The Pen Register*, 20 DRAKE L. REV. 108 (1970); Victor S. Elgort, *The Legal Constraints Upon the Use of the Pen Register as a Law Enforcement Tool*, 60 CORNELL L. REV. 1028 (1975); Clifford S. Fishman, *Pen Registers and Privacy: Risks, Expectations, and the Nullification of Congressional Intent*, 29 CATH. U. L. REV. 557 (1980).

¹⁹⁵ Ian C. Ballon, *E-Commerce and Internet Law: A Primer*, in *Fourth Annual Internet Law Institute* (Ian C. Ballon et al. eds., 2000) (citing *In Re: Amendments to Rule of Judicial Administration*, 651 So. 2d 1185 (Fla. 1995)).

¹⁹⁶ *Id.* at 128. (emphasis added).

¹⁹⁷ 18 U.S.C. § 2701 (2001).

¹⁹⁸ *Id.*

¹⁹⁹ Bertron, *supra* note 68, at 176.

²⁰⁰ *Id.* at 177-78.

²⁰¹ U.S. DEPARTMENT OF JUSTICE, *FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS* (July 1994) (supplemented in 1997 & 1999), available at <http://usdoj.gov/>

The Fifth Circuit has held that the term "intercept" means the acquisition of an electronic communication that is "contemporaneous with the transmission of those communications."²⁰² Steve Jackson Games ran a commercial bulletin board service on which players of their games could exchange information.²⁰³ The Secret Service suspected them of cyber-terrorism and hacking based upon one of the commercial role-playing games it marketed.²⁰⁴

In executing a search warrant authorizing seizure of "computer hardware . . . and computer software," the U.S. Secret Service searched, read, and deleted 162 items of unread, private e-mail stored on the BBS. Because the Secret Service obtained neither a court order to intercept, nor a warrant to search the stored communications, the Fifth Circuit upheld the district court's conclusion that ECPA had been violated and likewise affirmed a statutory damages award.²⁰⁵

The ECPA requires that if an electronic communication service has held the contents of an electronic communication in storage for 180 days or less, it may disclose that communication to the government only pursuant to a federal or state warrant.²⁰⁶ The Eleventh Circuit held in *Lopez v. First Union National Bank of Florida* that a verbal instruction by law enforcement was insufficient for disclosure of electronic wire-transfer records.²⁰⁷ However, it distinguished between documents in storage and those in transmission. Lopez's claim that the ECPA was violated when the Bank released communications in storage was dismissed.²⁰⁸

Alleging that First Union disclosed a communication held in "electronic storage," which violates § 2702(a)(1), is not equivalent to alleging that First Union disclosed a communication in "transmission," which would violate § 2711(3)(a). Because the complaint does not allege that First Union disclosed communications while in transmission, it fails to state

criminal/cybercrime/search_docs/toc.htm.

²⁰² Bertron, *supra* note 68, at 178 (quoting *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 459-60 (1994)).

²⁰³ *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (1994).

²⁰⁴ *Id.*

²⁰⁵ Bertron, *supra* note 68, at 178.

²⁰⁶ 18 U.S.C. § 2703(a) (2001).

²⁰⁷ *Lopez v. First Union Nat'l Bank of Fl.*, 129 F.3d 1186 (11th Cir. 1997). Pursuant to a seizure warrant, the bank provided "law enforcement authorities access to contents of the electronic funds transfers sent to Lopez that were being held in electronic storage." *Id.* at 1188.

²⁰⁸ *Id.* at 1189.

a claim under § 2711(3)(a).²⁰⁹

This distinction between storage and transmitted communications only adds to the confusion of which standard to apply to e-mail. Letters are treated the same whether they are being transported by the United States Postal Service or sitting stored within someone's personal desk. The courts, much like Congress, are unclear as to where this new medium should fall. Currently, the ECPA classifies e-mail as electronic communications subject to the same protections as telephone conversations. However, e-mail is not a phone conversation and the Carnivore system does more than a traditional pen register or trap and trace. The question then becomes whether such an interception should be subject to constitutional or statutory protections, and if it can successfully pass either.

VI. FULL CONTENT INTERCEPTIONS: A COMPARATIVE ANALYSIS

When law enforcement seeks to intercept the communications between two parties, it is limited by constitutional and statutory requirements. These procedures exemplify the level of privacy afforded to a particular means of communications and protect them from governmental intrusion. How much protection, however, depends upon the means of the communication rather than the substance.

The reason for this distinction rests historically in the technology. In general, written letters and papers constitute the original form of communication between people. Paper, as used here, includes one's diary, love letters, bills, and credit card statements. From the most mundane daily receipt to the most confidential personal record, paper plays a fundamental role in our lives and has done so since the invention of papyrus.

In contrast, telephone, faxes, the Internet, and e-mail are all relatively new phenomena. Only in the last century have individuals been able to transmit their voice (and consequently, their ideas) across space. Families once divided by geography can carry on close relationships. Friends converse even though living on separate continents. Business operates twenty-four hours a day due to the globalization of the economy, and information trades as a commodity. Electronic communications quicken the exchange of ideas, but do not fundamentally alter its content. Illogically, the courts do not agree. Traditional communication receives differing treatment under the law than new technologies. Consequently, burgeoning media such as electronic mail lacks fundamental privacy.

A. *Traditional Mail*

Philosophically and legally, traditional letters receive the highest level of

²⁰⁹ *Id.* at 1190.

protection from unwarranted searches and seizures. Explicit in the Constitution, personal papers are equivalent to an individual's home.²¹⁰ Intrinsically, documents that are drafted and mailed constitute the private thoughts of a citizen, and those thoughts are protected not only under the Fourth Amendment, but also the First and Fifth Amendments.²¹¹

Samuel Warren and Louis Brandeis argued in their seminal essay on the right to privacy that the "principle which protects personal writings and any other production of the intellect or of the emotions, is the right to privacy. . . ."²¹² Mental works implicitly represent the belief that the creator has control over their dissemination. Protection from public disclosure of private facts is an essential element of the right to privacy.²¹³ Both explicitly and implicitly, the law protects papers and thus letters from invasion. Individuals have always expected, and continue to expect, that their personal ideas will not be made known to others without their consent or court intervention.

Because of this perception, the mail receives the highest level of protection of all forms of communications. A search of the mail requires a valid warrant. In order to obtain such a warrant, law enforcement must show by oath or affirmation probable cause such that exists when "the facts and circumstances within . . . [the officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that' an offense has been committed."²¹⁴ Furthermore, the warrant must state with specificity the place to be searched and things to be seized, and must be signed by a detached and neutral magistrate.²¹⁵

These stringent procedural requirements protect letters from overzealous and arbitrary searches. The probable cause standard requires more than a mere suspicion of wrongdoing, thus protecting citizens from random searches. Furthermore, requiring a judicial officer to issue the warrant affords an external check on law enforcement activities. A detached third party must review the information provided by investigators and determine whether it is sufficient to invade an individual's privacy.

In addition to these procedures, the most important component of the jurisprudence protecting full content searches of mail is the exclusionary rule. The right to have one's personal affects protected would be meaningless without some

²¹⁰ U.S. CONST. amend. IV; *Olmstead v. United States*, 277 U.S. 438 (1928).

²¹¹ U.S. CONST. amends. I, V (protecting freedom of speech and right against self incrimination respectively).

²¹² Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213 (1890).

²¹³ William Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

²¹⁴ *Brinegar v. United States*, 338 U.S. 160, 175-76 (1949) (quoting *Carroll v. United States*, 267 U.S. 132, 162 (1925)).

²¹⁵ *Johnson v. United States*, 333 U.S. 10, 14 (1948).

remedy. When officers violate the search warrant requirements set forth above the evidence wrongfully obtained is excluded from admission into evidence.²¹⁶ This helps to ensure against wrongful activity by police. If there were no consequences for obtaining evidence in violation of the Fourth Amendment, there would be no incentive to act within the bounds of the Constitution. Thus, mail receives a multitude of constitutional protections equal to those of homes. Contrast this with the lower levels of protection granted electronic communications.

B. *Electronic Communications*

Unlike papers, electronic communications have not enjoyed implicit or explicit protections against unwarranted searches and seizures. To the contrary, the courts originally found no privacy whatsoever in conversations transmitted over telephone lines.²¹⁷ Privacy depended on some physicality which mere conversations lacked. The trespass doctrine relied upon the intrusion of a person's home, a constitutionally protected area.²¹⁸ Conversations were protected not on the grounds that they were inherently private, but on where they were intercepted.²¹⁹

The Constitution makes no explicit mention of protecting conversations and the Supreme Court for many years refused to expand the Fourth Amendment to do so.²²⁰ The right to privacy that communications now enjoy has developed over time, rather than being inherent in peoples' conceptions of them. This contrasts starkly with the fundamental belief that privacy extends to a person's papers.

The philosophical underpinning of communications surveillance rests upon propertied interests, and the Court has struggled with its application to oral and wire communications. This difficulty only multiplies when the means of communications are electronic. Cyberspace consists of no tangible property; instead, it is an amalgam of thoughts, conversations, records, and intellectual property. This lack of tangibility delineates it even further from the legal reasoning extending privacy protection to telephone conversations. Furthermore, communication technology continues to change forcing the courts to play a losing game of catch-up.

Although oral and wire communications now receive full constitutional and statutory protections,²²¹ electronic communications have not been afforded this same treatment. E-mail may be intercepted pursuant to a warrant issued not by a

²¹⁶ *Weeks v. United States*, 232 U.S. 383 (1914).

²¹⁷ *See Olmstead v. United States*, 277 U.S. 438 (1928).

²¹⁸ *Boyd v. United States*, 16 U.S. 616, 627 (1886).

²¹⁹ *Olmstead*, 277 U.S. at 464.

²²⁰ *Id.* at 465.

²²¹ *See* 18 U.S.C. §§ 2510-2520 (2001); *Katz v. United States*, 389 U.S. 347 (1967).

court order, but rather by the authorization of an attorney general.²²² In addition, the ECPA explicitly does not apply the exclusionary rule to illegal interceptions of e-mail.²²³

This differential treatment subjugates e-mail to a lesser form of communication. It eliminates the external check and remedy afforded to traditional papers. It makes little sense to protect papers based on format. For example, suppose an individual writes a personal letter to their spouse or doctor about something of great importance. In one case, that person places the letter in an envelope, seals it, and sends it along its way via post or merely leaves it on her desk. The information contained in that piece of paper would receive the highest form of protection afforded under the Fourth Amendment.

In the other instance, the individual scans the document into a computer (or, more likely, has drafted it on one) and e-mails it to the same addressees to whom the hard copy is going. The manner in which she chose to send the document greatly compromises the protection it will be granted. Law enforcement may more easily intercept the electronic copy under statutory provisions of Title III.²²⁴ Also, in the event that the information has been obtained in violation of these requirements, there is no recourse, other than a civil action, to remedy the wrong.²²⁵

The differential treatment rests upon a fundamental misunderstanding of the technology. The purpose and substance of online communications is identical to that of traditional paper. The distinction rests upon the medium alone and should be eradicated. As individuals increase their reliance on electronic communications for all functions of daily life, they will concomitantly increase their expectations of privacy in these mediae. It is imperative that the law value substance over form and recognize a right to privacy inherent in all forms of communication.

VII. PARTIAL CONTENT INTERCEPTIONS: A COMPARATIVE ANALYSIS

Both pen registers and mail covers effectively achieve the same goal: they allow law enforcement to gain the information on the outside of a communication to determine its origin and destination. Pen registers and trap and trace electronic listening devices provide information about the digital tones that constitute a phone number. Mail covers include the address and postmark information on the outside of standard domestic correspondence. Neither provides any specific information

²²² See Steere, *supra* note 170, at 252.

²²³ *Id.*

²²⁴ 18 U.S.C. §§ 2510-2522 (2001).

²²⁵ *Id.*

about the contents of a package other than that which is readily ascertainable.²²⁶

These types of general address searches receive less Fourth Amendment protection than full content searches of electronic communications. This distinction again rests on the reasonable expectation of privacy test articulated in *Olmstead*.²²⁷ Because it is assumed that others must read the information for transmission, the sender must have a diminished expectation of privacy. After all, the person chooses who and how to send the message.

A. *Mail Covers*

Law enforcement may conduct a mail cover search under reasonable suspicion for four specific purposes.²²⁸ The search does not require independent authority; rather, only the approval of a postal inspector is necessary.²²⁹ Therefore, subject to only limited exceptions, law enforcement may obtain all of the mailing information of an individual. This could include the size, weight, and destination of all packages or letters being sent. In addition, all shipments incoming may be observed and inventoried.

Again, the general reasoning behind this is that people have no expectation of privacy in addressing information. However, the Court ignores the expectation of privacy people have in what comes in and out of their home. When a citizen puts a parcel in the hands of the United States Postal Service, they expect that a mail clerk will necessarily read the outside of the package. It is unlikely, however, that they anticipate a police officer would observe and record that same information. The same could be said of telephone calls coming in and out of an individual's home.

B. *Pen Registers and Trap and Trace Devices*

Like mail covers, pen registers are afforded few constitutional protections. Law enforcement may conduct such a search under authorization of any court after showing its relevancy to an ongoing investigation.²³⁰ This diminished standard allows for interception of all numbers dialed without any showing of probable cause. In contrast, such a tap might not even be put on a suspect's phone, but rather on a friend's or family member's phone regularly used by the target of the

²²⁶ Cf. *United States v. Jacobsen*, 466 U.S. 109 (1983) (holding that the search of a package which was visibly leaking cocaine did not constitute a "search" within the meaning of the Fourth Amendment).

²²⁷ *Olmstead v. United States*, 277 U.S. 438, 468 (1928).

²²⁸ 39 C.F.R. § 233.3(e)(2) (2001).

²²⁹ 39 C.F.R. § 233.3(d) (2001).

²³⁰ 18 U.S.C. §§ 3122-3123 (2001).

investigation. This enables law enforcement to ascertain the full list of people called from a certain telephone number.

The Court reasoned that individuals have no privacy expectation in such information.²³¹ If this were the case, would the justices not mind having a list of all the numbers that they dialed within the past month published in the *Washington Post*, or better yet placed into an FBI file? Most people probably do expect the phone number and identities of those they call to remain private. That type of information reveals more than just a series of numbers. It describes habits, propensities, relationships, and quirks. Numbers of mistresses, shops, and 1-900 services may reveal more about an individual than other investigative techniques subject to full Fourth Amendment protections.

These types of address interceptions receive less protection because of diminished privacy expectations. They should, however, receive the full Fourth Amendment protection afforded to content interceptions. The question then becomes where does an e-mail interception like those conducted under *Carnivore* fall? Should it receive full content protection, or is it more analogous to a partial interception? Finally, what procedures currently govern the use of *Carnivore*, and do they rise to the appropriate standard?

VIII. CARNIVORE: A HYBRID

Utilizing *Carnivore*, law enforcement may intercept the routing information contained in an electronic mail communication. This information, consisting of binary data, reveals the e-mail address of the sender and receiver, date, time, and the subject line. The last of these may consist of as much or as little information as the sender wants. Sometimes it is left completely blank, but others may contain specific information including attachment file names.

As such, the information contained in e-mail addresses does not easily fall into either category of analysis: traditional or oral. No case law yet exists on the searches of e-mail addresses. By way of analogy, the courts will surely treat it as a pen register and protect it accordingly. E-mail jurisprudence has applied the law of oral communications, and both are protected under Title III. Therefore, the obtaining of binary code constituting address information would be comparable to the interception of digital dial tones that make up a telephone number.

The distinction, however, is that *Carnivore* does more than that. *Carnivore* can and does reveal the subject matter line of an e-mail. The Court pointed directly to the fact that no information was intercepted using a pen register in *New York Telephone*.²³² It stated: "[N]either the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even

²³¹ *Smith v. Maryland*, 442 U.S. 735 (1979).

²³² *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 167 (1977).

completed is disclosed by pen registers.”²³³ That is not the case with e-mail interceptions.

The subject matter line does reveal the purport of the communication. In fact, it states explicitly the purpose of the letter. In contrast, a phone call may contain no content at all if it is not completed. Calls might be wrong numbers or the desired person may not be home. An e-mail address contains who is doing the writing and the name of the recipients. The entirety of the communication may be contained within the single message — a stark contrast to a number dialed.

E-mail has a self-contained nature. Within it are all the contents that it will ever have, and Carnivore possesses the capability to intercept it.²³⁴ Because of this, Carnivore should be subject to full content protections rather than the standard of either a mail cover or pen register. In this instance, the potential reach of law enforcement is far too great. It has both the capability and freedom to intercept large amounts of information based on little more than relevancy. This power must be weighed against the privacy rights inherent in communication of documents. Thus, the full warrant requirement and exclusionary rule must be applied to any searches conducted with the Carnivore program.

IX. CARNIVORE: THE CURRENT STANDARDS AND THEIR ADEQUACY

The FBI has established standards governing the use of Carnivore, and they follow those established by the ECPA. First, it must demonstrate probable cause to a judicial authority.²³⁵ Second, it must explain why traditional enforcement methods are insufficient.²³⁶ Finally, the Bureau looks at the size of the ongoing investigations and the resources spent on conducting electronic surveillance.²³⁷

These standards rise to the level of those established under traditional constitutional and statutory protections. They do not, however, extend the exclusionary rule to improper interceptions. This is something that remains for the Court to decide. Hopefully, it will recognize the lack of distinction between an electronic messages and physical paper and afford the former the same level of protection as the latter.

X. CONCLUSION

The law governing the search and seizure of communications is vast and complex. This is due in large part because courts insist on relying on outdated

²³³ *Id.*

²³⁴ *See* Poulsen, *supra* note 4.

²³⁵ Motta, *supra* note 8 at 665.

²³⁶ *Id.*

²³⁷ *Id.*

definitions of communications. When the Fourth Amendment sought to protect "houses, papers, and effects,"²³⁸ it meant that protection to be present regardless of the form those items take. Papers are the private communications of individuals whether they are written on parchment, stationery or in the bits of data that constitute this document.

The Carnivore initiative represents another attempt by law enforcement to control crime in cyberspace. It appears that the FBI understands the concerns of privacy advocates and has implemented a procedure that mirrors the protections currently provided under the law. Unfortunately, that law does not recognize that as science advances, new communications technologies will continue to replace the old while long-understood expectations of privacy will spill into the brave new world.

Sandy D. Hellums

²³⁸ U.S. CONST. amend. IV.