12-1-2005

# Fourth Amendment Protection from Government Intrusion of E-mail and Internet Communications

William Randall King
*Georgia State University College of Law*

Georgia State University | COLLEGE OF LAW

Research Guides

# Fourth Amendment Protection from Government Intrusion of E-mail and Internet Communications

### Guide Information

| | |
|---|---|
| Last Updated: | Oct 29, 2010 |
| Guide URL: | http://libguides.law.gsu.edu/fourthamendmentemailprotection |
| Description: | William Randall King - Fall 2005 - Constitutional; Technology Law; Privacy Law |
| Tags: | constitutional_law, privacy_law, technology_law |
| RSS: | Subscribe to Updates via RSS |

### Guide Index



## Introduction

### Overview

This website provides a research guide for the analysis of Fourth Amendment protection from governmental intrusion on personal e-mail and Internet communications. The scope of this research guide is limited to protection of the Fourth Amendment provides as to acts of government agencies and law enforcement officials in obtaining e-mail and Internet communication data, either through real-time interception or retrieval from electronic storage. This research guide does not provide a detailed history of the evolution or application of the Fourth Amendment to the Constitution of the United States, nor does it deal with the establishment or violation of rights to privacy from the intrusion by non-governmental agencies such as employers or other private citizens.

As you will find below, there are no authoritative or landmark cases that pass on the reasonable expectation of privacy a person has in their Internet communication. Most analysis of the Fourth Amendment protection in cases and legal articles or publications analogize the nature of an e-mail or web communication to several categories of traditional forms of communication on which the court has already ruled or for which the statutory provisions specifically allow. This often involves whether the communication was intercepted in real-time, which the courts regard like a traditional telephone conversation, or extracted from "electronic storage", which is considered more like personal papers and effects. The level of protection afforded also depends on whether the storage is short term, which the courts have analogized to a safety deposit box, or long term which has been treated like filed business papers.

The amount of information intercepted from an e-mail or Internet communication also plays a major part in the determination of the Fourth Amendment protection, where the courts have found an expectation of privacy in the “content” of a communication, but not in the “dialing, routing, addressing, and signaling” information that accompanies the communication. Thus interception of this adjunct routing information does not constitute a search under the Fourth Amendment at all.

This treatment of the Fourth Amendment application to e-mail and Internet communications does not provide an easy method for determining the level of protection to be afforded a particular intercepted e-mail or Internet communication by the courts. While this research guide does not assume to suggest the proper answer to this question, it does seek to expose the reader to the many facets of analysis required to argue the issue from either side.

### About the Author

William R. King is a second-year law student at Georgia State University College of Law and Moot Court board member. William's interests lie in technology related law, including Intellectual Property, e-Commerce, and Internet privacy issues.

### Disclaimer



Back to Top

# Primary Sources

## Constitution

The Fourth Amendment to the constitution clearly establishes the concept that a "reasonable" search requires a warrant supported by probable cause, and this concept has been vigorously applied by the courts in all but a few exceptional circumstances, e.g. when the immediacy of the search is necessary to protect the life of the officer or others, or when there is the pending danger that evidence may be destroyed. Often, the question turns not on the reasonableness of the search, i.e. the validity of the warrant, but on whether the intrusion constitutes a search under the Fourth Amendment at all.

| | |
|---|---|
| U.S. CONST. amend. IV. | 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. |

## Legislative Acts

The following legislative acts represent Congress' will to provide protection for the privacy of electronic communications. However, the protection provided in these statutes often criminalizes the intrusion upon personal e-mail or Internet by private citizens while at the same time lowering or circumventing the Fourth Amendment protection against the same intrusion by the Government.

| | |
|---|---|
| Title III of the Omnibus Crime Control And Safe Streets Act Of 1968, Pub. L. No. 90-351; 82 Stat. 197 (1968). | Title III of the Omnibus Crime Control And Safe Streets Act Of 1968, or the Wiretap Act, enacted by Congress under the guidance of the Katz and Berger decisions, established strict limitations on the Government's ability to intercept oral communications transmitted over wire. A Wiretap warrant required a high level of scrutiny by the issuing court (often referred to as super warrant requirements), detailing the conversations to be intercepted and the persons for whom conversations were sought. Wiretaps were to be used as a last resort investigative technique and were required to be terminated immediately once the specified information was obtained. The relevant provisions are codified at 18 U.S.C. §§ 2510-22. |
| Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986). | The Electronic Communications Privacy Act of 1986, or ECPA, expanded the statutes promulgated under the Wiretap Act to include non oral and non-wire based electronic communications. The ECPA also established protection for electronically stored information, such as documents stored in computer files codified in 18 U.S.C. §§ 2701-12.<br><br>Further, the Legislature, apparently in response to the Court's decision in *Smith v. Maryland*, established in the Act rules and requirements for the installation of pen register devices, including the requirement of a court order, albeit a lesser requirement than a warrant supported by probable cause. These provisions are referred to as the Pen Register statutes and are codified in 18 U.S.C. §§ 3121-27. |
| Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). | In response to the terrorist attacks on September 11th, the Congress enacted the USA PATRIOT Act, or Patriot Act. This act amended several statutes promulgated by the Wiretap Act and ECPA, such as amending the definition of a wire communications in 18 .U.S.C. 2510(1) so that it would no longer include such communications when in electronic storage, thus allowing the government to obtain voicemail communications under the less restrictive standards of these statutes.<br><br>The Patriot Act also expanded the definition of pen register and trap and trace devices in 18 U.S.C. § 3127(3)-(4) to include dialing, routing, addressing, and signaling information to make the devices more readily applicable to modern forms of electronic communication, such as the Internet. The Act further modified the Pen Register statutes to ensure that any devices utilized under the statute would not intercept "content" information and the law enforcement officers would use all technology reasonably available to prevent the interception of content in 18 U.S.C. § 3121. |

## Statutes

While the operable body of statutory law for the protection of privacy in electronic communications is contained in the entire sequence of statutes promulgated by the legislative acts above, the following excerpts have been provided that are specifically applicable to the protection of personal Internet communications from Governmental intrusion.

| | |
|---|---|
| 18 U.S.C. § 2510(8) (2005). | "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; |
| 18 U.S.C. § 2518(1) (2005). | (1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:<br>(a) the identity of the investigative or law enforcement officer making the application, and the |

| | |
|---|---|
| | officer authorizing the application;<br>(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;<br>(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;<br>(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;<br>(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and<br>(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results. |
| 18 U.S.C. § 2703(a)-(b) (2005). | (a) Contents of wire or electronic communications in electronic storage. A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.<br><br>(b) Contents of wire or electronic communications in a remote computing service.<br>(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--<br>(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or<br>(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--<br>(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or<br>(ii) obtains a court order for such disclosure under subsection (d) of this section;<br>except that delayed notice may be given pursuant to section 2705 of this title.<br>(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--<br>(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and<br>(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing. |
| 18 U.S.C. § 2703(c) (2005). | (c) Records concerning electronic communication service or remote computing service.<br>(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--<br>(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;<br>(B) obtains a court order for such disclosure under subsection (d) of this section;<br>(C) has the consent of the subscriber or customer to such disclosure; or<br>(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title; or<br>(E) seeks information under paragraph (2).<br>(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--<br>(A) name; |

| | |
|---|---|
| | (B) address;<br>(C) local and long distance telephone connection records, or records of session times and durations;<br>(D) length of service (including start date) and types of service utilized;<br>(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and<br>(F) means and source of payment for such service (including any credit card or bank account number),<br>of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).<br>(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer. |
| 18 U.S.C. § 3121(c) (2005). | (c) Limitation. A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications. |
| 18 U.S.C. § 3122 (2005). | Application for an order for a pen register or a trap and trace device<br><br>(a) Application.<br>(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.<br>(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.<br><br>(b) Contents of application. An application under subsection (a) of this section shall include--<br>(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and<br>(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency. |
| 18 U.S.C. § 3127(3)-(4) (2005). | (3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;<br><br>(4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication; |

## Cases

### Expectation of Privacy

Up until 1967 the courts had treated current day electronic communications, i.e. the telephone, like any other personal papers and effects under the line of cases established by *Olmstead v. United States*, 277 U.S. 438, and *Goldman v. United States*, 316 U.S. 12. Specifically, for a violation of Fourth Amendment protection from the interception of a telephone conversation to be established, it was necessary for a trespass to have occurred. By 1967 the Supreme Court recognized the importance that the telephone had acquired in American's daily lives, and sought to establish new boundaries for the protection of the public's use of this now pervasive form of communication.

| | |
|---|---|
| *Katz v. United States*, 389 U.S. 347 (1967). | This case involved the a phone conversation of the defendant intercepted from a public phone booth by the planting of an electronic "bug" on the outside of booth by the law enforcement officer without first obtaining a warrant.. The Court held that the Fourth Amendment protects people not places, and abandoned the requirement of trespass for a government action to be a search under the Fourth Amendment in favor of the reasonable expectation of privacy test.<br><br>*Katz* is also significant in this context because it dealt with the interception of a telephone conversation. The Court recognized the difference between an aural conversation and more tangible papers and effects, and sought to provide the proper level of protection for such intangible communications under the Fourth Amendment. |

| | |
|---|---|
| *Berger v. New York*, 388 U.S. 41 (1967). | This case dealt with the constitutionality of a State eavesdrop statute, N.Y. CRIM. PROC. CODE § 813-a. The Court held that the statute violated the Fourth Amendment by allowing an intrusion into the privacy of the defendant without a warrant supported by probable cause or describing the particular conversations to be intercepted.<br><br>The Court in *Berger* laid out detailed requirements for a warrant authorizing electronic surveillance, including the identification of the conversations and the person whose conversations were sought, and required that electronic surveillance investigations be no longer than necessary to obtain the sought-after information, after which they must be terminated. The Court stressed the need for "adequate judicial supervision or protective procedures" over the issuance and performance of surveillance warrants. These restrictions provided guidance to the "super warrant" requirements that the legislature drafted into the Wiretap Act. |

Up to the writing of this research guide, there has been no Federal case law which passes on the reasonable expectation of privacy in e-mail or other personal Internet communication. A few non-federal jurisdiction cases are noteworthy, however.

| | |
|---|---|
| *United States v. Maxwell,* 45 M.J. 406 (1996). | This case involved the violation of the defendant of the U.C.M.J. by the exchange of pornographic images over the internet and the use of indecent language via email. A warrant was obtained to retrieve the obscene graphic files from the service provider (AOL), but did not specifically include specification that the emails should be obtained.<br><br>The Court held that the retrieval of the emails without proper specification in the warrant violated defendant's Fourth Amendment rights and therefore reversed defendant's conviction as to the obscene languages.<br><br>Notable to our context here is the Court's recognition that an individual has a reasonable expectation of privacy in e-mails stored on an ISP's computers, analogizing e-mails to phone conversations and sealed letters. |
| *Commonwealth v. Proetto*, 771 A.2d 823 (Pa. Super. Ct. 2001). | In this case the defendant made sexually explicit remarks to a child via Internet chat and sent a sexually explicit picture to her via e-mail. The defendant attempted to suppress the evidence based on his Fourth Amendment right to privacy in his communications.<br><br>The Court held in this case that defendant had no reasonable expectation of privacy in e-mail and Internet communications because the defendant had no way of knowing who was on the other end of the communications, and that those communications were not protected by the Fourth Amendment. Further, since the e-mails and chat transcripts were recorded on the receiving in and turned over to the police, the communications were not intercepted "contemporaneous with the transmission", there was violation of the Pennsylvania Wiretapping and Electronic Surveillance Act (similar to the Wiretap Act). |

Electronic Storage

The Electronic Communication Privacy Act (ECPA) in 1986 added statutory provisions to the U.S. Code dealing with electronic communications and transactional records residing in electronic storage. Specifically, the statute provides the methods by which the government may obtain communications and records from electronic communication service providers in 18 U.S.C. § 2703.

While targeted at traditional computer files, this statute becomes applicable to e-mail communications through the technical nature of the transmission of an e-mail. As the e-mail is routed through the various devices and computers that make up the communication channel, it is often stored and then retransmitted. Thus an e-mail exists simultaneously as a live communication deserving of the heightened protection afforded a telephone conversation and as a communication in electronic storage which has traditionally been afforded much less protection.

While many of the following cases deal with civil matters, they reveal the courts' struggle with this duality.

| | |
|---|---|
| *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994). | In this case, the Secret Service seized a computer from a service provider that contained, among other things, the e-mails of 365 customers.<br><br>The Court held that this seizure of the e-mails was a violation of Title II of the ECPA dealing with stored wire and electronic communications, 18 U.S.C. § 2701 et. seq., but no a violation of the Wiretap Act and subsequent amendments under 18 U.S.C. 2510 et. seq., because violation of the Wiretap Act required interception of the e-mail to be "contemporaneous with transmission", or intercepted real-time. |
| *Konop v. Hawaiian Airlines*, 236 F.3d 1035 (9th Cir. 2001). | This case involved an airline pilot who's website had been illegally accessed by his employer who obtained e-mails sent by the plaintiff critical of his employer. Plaintiff pushed for seizure of the e-mails to be a violation of the Wiretap Act, 18 U.S.C. 2510 et. seq. as opposed to Title II of the ECPA, 18 U.S.C. § 2701 et. seq. because of the increased civil damages available for intercepted communications as opposed to those retrieved from electronic storage.<br><br>This case is notable in our analysis because the Court recognized the dual nature of an e-mail communication, stating "an electronic communication in storage is no more or less private than an electronic communication in transmission. Distinguishing between the two for purposes of |

| | |
|---|---|
| | protection from interception is irrational and an unsupportable result given Congress' emphasis of individual privacy rights during passage of the ECPA."<br><br>However, the Court's decision was subsequently withdrawn, and a new decision issued that followed *Steve Jackson Games* requirement that an interception must be contemporaneous with the e--mail's transmission. |
| *United States v. Councilman*, 373 F.3d 197 (1st Cir. 2004). | In this case a company who provided book publishing services and communication services to book sellers implemented a system to intercept the e-mail messages of its customers to gain a competitive advantage.<br><br>The court recognized that e-mails traveling the Internet may "constantly" be in storage and in transit "simultaneously", but they found that in this case the technical nature of the interception took place during temporary, intermediate storage of the message and not "while in transmission through the wires or cables between computers", and that therefore the plaintiffs were foreclosed from their claims under the Wiretap Act, 18 U.S.C. 2510 et. seq. |

### Information Voluntarily Conveyed to 3rd Parties

In determining whether certain information intercepted from personal Internet communications was deserving of Fourth Amendment protection, the courts may apply previous holdings that a person has no expectation of privacy in information voluntarily conveyed to a third party . This factor was instrumental in the Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), which established the basis for the use of pen register devices by law enforcement without a warrant supported by probable cause.

This doctrine would be most applicable to e-mail communications received by the intended recipients, thus terminating the senders expectation of privacy. *United States v. King*, 55 F.3d 1193, 1196 (6th Cir. 1995). Also falling under this doctrine are portions of e-mail or web communications required for the Internet service provider (ISP) to fulfill the desired request, i.e. sending the e-mail or retrieving the requested web document, and may include e-mail addresses, web addresses, etc. from the communication. This doctrine has also been applied to personally identifiable information provided to an ISP in establishing a service account and subsequently obtained by law enforcement officers in relation to a specific communication or set of communications.

| | |
|---|---|
| *United States v. Miller*, 425 U.S. 435 (1976). | Account records obtain from defendant's banks were used to convict defendant of a variety of charges of illegal manufacturing of whiskey and tax fraud. The defendant contended that the seizure of the bank records violated his Fourth Amendment rights.<br><br>The Court established that the defendant had no legitimate expectations of privacy in his bank records because the bank was a third party to which he disclosed his affairs when he opened his accounts at the bank, and that therefore no Fourth Amendment protection existed. |
| *Smith v. Maryland*, 442 U.S. 735 (1979). | The defendant was convicted of robbery in part based on evidence obtained by the installation of a pen register device to record the phone numbers dialed from defendant's home.<br><br>The Court held that the defendant had no reasonable expectation of privacy in the digits dialed into his phone in part because this information was voluntarily conveyed to the phone company and used by the phone company in the normal course of business, such as establishing communications, billing, and detecting and preventing obscene or annoying callers. |
| *United States v. Hambrick*, 55 F.Supp.2d 504 (4th Cir. 2000). | An undercover officer determined from online conversations with the defendant that the defendant intended to entice a minor child to leave his home and come and live with defendant. The officer seized records from the defendants Internet service provider (ISP) that allowed the officer to identify defendant.<br><br>The Court held, that while the subpoena used to obtain the records was invalid, that the defendant nevertheless had no expectation in the privacy of the information he conveyed to his ISP ant therefore was entitled to no protection under the Fourth Amendment. |
| *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001). | Law enforcement agents seized computers from the operator of a BBS which contained, among other things, the e-mails of the board's subscribers. The subscribers claimed that the seizure of their e-mails violated their Fourth Amendment rights.<br><br>The Court held that the subscribers lost their legitimate expectation of privacy in any e-mail that had already reached its recipient; analogizing these facts to a letter-writer, whose "expectation of privacy ordinarily terminates upon delivery" of the letter. |
| *United States v. Butler*, 151 F. Supp. 2d 82 (D. Me. 2001). | A student was charged with illegally receiving child pornography over University computers in part on evidence obtained from "session logs" maintained by the University which identified the defendant as recipient of the computers. The defendant moved to suppress claiming that seizure of the session logs violated his Fourth Amendment rights.<br><br>The Court held the defendant had not established a reasonable expectation of privacy in the session logs, since the logs were obviously maintained for the benefit of the University and not the defendant, and therefore were suppressible on the defendant's motion. |

### Content vs. Routing/Addressing Information

The statutory language promulgated by the legislature in the acts detailed below define a distinction between the "content" of a communication, for which a warrant supported by probable cause is required for interception under the Wiretap Act, and dialing, routing, addressing, and signaling information, which can be intercepted under the Pen Register statute promulgated by the ECPA by simply showing that some information relevant to an ongoing investigation is likely to be revealed. 18 U.S.C. § 3122(b)(2).

The application of this distinction to e-mail and Internet communications becomes problematic, because e-mail addresses and web site URLs, while used to establish communication like a phone number, also relay much more information about the purpose of the communication and the identity of the parties involved in the communication.

The difference in Fourth Amendment protection afforded these two components of a communication and the related policy was established in the following cases.

| | |
|---|---|
| *United States v. New York Tel. Co.,* 434 U.S. 159 (1977). | The plaintiff phone company challenged a court order for the installation of pen register devices on the phones of alleged gambling enterprise, claiming that the devices could only be installed pursuant to the Wiretap Act, 18 U.S.C. § 2510 et. seq.<br><br>The Court held that the installation of the pen registers was not governed by the Wiretap Act because they did not intercept the content of the communication as defined in 18 U.S.C. § 2510(8), noting that "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". |
| *Smith v. Maryland*, 442 U.S. 735 (1979). | The defendant was convicted of robbery in part based on evidence obtained by the installation of a pen register device to record the phone numbers dialed from defendant's home.<br><br>The Court held that the defendant had no reasonable expectation of privacy in the digits dialed into his phone in part because the digits were simply a means of establishing communication and did not reveal any "content" of the phone conversation. |

Back to Top

## Secondary Sources

### Books and Treatises

The following books and treatises on the subject are available and are quoted or cited in the various law review articles and publications referenced in this research guide.

| | |
|---|---|
| Technology and Privacy: The New Landscape (Philip E. Agre & Marc Rotenberg eds., 1997) | This book contains a series of 10 scholarly essays on technology-based privacy issues. Each essay provides addresses the current state of privacy and the direction things are headed. The most prevalent theme in the essay is how advances in cybertechnology have led to greater threats to personal privacy, but have also led to greater promise for privacy protection. |
| Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age (2004). | This book by Daniel, an associate law professor at George Washington University Law School, provide insight into the current state of privacy in American, including the constant collection of personal data gleaned from our Internet surfing into "digital dossiers" which pose a grave threat to our privacy and recommendations on how the law can be reformed to simultaneously protect our privacy and allow us to enjoy the benefits of our increasingly digital world. |
| Robert O'Harrow, No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society (2005). | Robert O'Harrow, who covers privacy and technology issues for the Washington Post, provides a detailed look at the growth of the surveillance industry from both the perspective of the corporations amassing of data marketing purposes to the government's push for surveillance in a post 9/11 world. |

### Online Research

The following websites can provide additional resources or search facilities to further research Fourth Amendment Protection from Governmental Intrusion of e-mail and Internet communications.

Westlaw makes a vast online library of legal research materials available to subscribers at http://www.westlaw.com.

Westlaw key numbers for researching Fourth Amendment protection of personal e-mail and Internet communications:

349 Searches and Seizures
349I In General
349k25 Persons, Places and Things Protected
349k26 k. Expectation of Privacy.

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General

372k1435 Acts Constituting Interception or Disclosure
372k1439 k. Computer Communications.

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1440 k. Persons Concerned; Consent.

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1475 k. Carrier's Cooperation; Pen Registers and Tracing

The U.S. Government Printing Office provides free access to Legislative, Executive, and Judicial materials, including the statutes and legislative acts referenced in this research guide, at http://www.gpoaccess.gov.

The Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice provides a website with articles and guides for law enforcement officers, parents, teachers, lawyers, victims of crimes, and citizens interested in combating computer and intellectual property crimes at http://www.cybercrime.gov.

The ACLU provides a website dedicated to Privacy and Technology Issues at http://www.aclu.org/Privacy/PrivacyMain.cfm.

Google provides a powerful and comprehensive web search capability at http://www.google.com.

Search keywords that will provide results relevant to Fourth Amendment protection of personal e-mail and Internet communications: *Smith Katz e-mail Internet Fourth Amendment expectation privacy*

## American Law Reports

The following *American Law Reports* annotations provide discussion of the applicable statutes and case law .

| | |
|---|---|
| Mitchell Waldman, *Expectation of Privacy in Internet Communications*, 92 A.L.R.5th 15 (2005). | This annotation collects and discusses cases dealing with the constitutional expectation of privacy in Internet communications. In the context of this research guide, the annotation deals specifically with electronic communications in transmission and does not include cases or decisions related to electronic storage.<br><br>The summary for the annotation provides the consensus result: "An expectation of privacy has generally not been found to exist with regard to subscriber information provided by service users to their Internet service providers, records on individuals' Internet usage, or as to communications made on Internet websites. Nor, with limited exception, have courts generally found a reasonable expectation of privacy to exist in e-mail or electronic chat-room communications." |

## Other Secondary Sources

These publications represent the attempt of other lawyers, academics, and law enforcement officials to distill the applicable law from the various statutes, case law, and doctrines that have been discussed to this point.

| | |
|---|---|
| James Adams, *Suppressing Evidence Gained by Government Surveillance of Computers*, 19 Crim. Just. 1 (Spring 2004 ), *available at* http://www.abanet.org/crimjust/cjmag/19-1/surveillance.html. | This article discusses what kinds of digital data gained by government surveillance can be used in court and how such information might be suppressed under the context of the doctrines referenced within this research guide. |
| Bradley J. Bennett , *Smith Meets The Patriot: The Digitization of The Pen Register Statutes And The Question of "Content"* (April 2, 2002) *at* http://www.uiowa.edu/~cyberlaw/cls02/bbennet1.html. . | This article looks at the effects of § 216 of the Patriot Act, specifically at how it modified the Pen Register provisions of the ECPA and how it effectively expands the Smith doctrine to include routing and addressing information from e-mail and other forms of Internet communication. This article also covers how the ECPA Pen Register statute as amended by the Patriot Act fits with FBI's Carnivore system for Internet surveillance. |
| U.S. Dep't of Justice, Criminal Div., *Searching and Seizing* | This document is a guide to law enforcement officials |

| | |
|---|---|
| *Computers and Obtaining Electronic Evidence in Criminal Investigations* (2002), *available at* http://www.cybercrime.gov/s&smanual2002.htm. | detailing legal issues which arise in searching and seizing computers and related electronic evidence in criminal investigations. The document outlines the applicable statutory rules and restrictions of various types of surveillance, details proper warrant application requirements, and provides guidelines for determining whether a particular type of information constitutes "content" for the application of the various statutes. |

### Law Reviews

The following law review articles provide detailed analysis of the case law and statutes presented in this research guide and were the source of much of the annotation and comments contained herein.

| | |
|---|---|
| Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9 (2004). | This article provides a detailed history of the acts and judicial decisions that make up the current "chaos" surrounding privacy and Fourth Amendment protection of online communications. |
| Robert Ditzion, *Electronic Surveillance In The Internet Age: The Strange Case Of Pen Registers*, 41 AM. CRIM. L. REV. 1321 (2004). | This article provides analysis of the distinction of content from dialing, addressing, routing and signaling information as applied to e-mail and Internet communications data in the context of the Pen Register statute as amended by the Patriot Act. |
| Deirdre K. Mulligan, *The Future Of Internet Surveillance Law: A Symposium To Discuss Internet Surveillance, Privacy & The USA Patriot Act: Surveillance, Records & Computers: Reasonable Expectations In Electronic Communications: A Critical Perspective On The Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004). | This article discusses the protection of privacy the ECPA as affords to electronic communications in the various categories discussed above, including additional distinctions specified in the act, e.g. in transmission, in "electronic storage" at a "electronic communication service" as opposed to a "remote computing service", etc. |

Back to Top

## Conclusion

### Conclusion

As we have seen, no landmark case nor general consensus exists that a person has a reasonable expectation of privacy in their e-mail and Internet communications.

The level of protection to be afforded a particular communication depends on a variety of facts, such as how the communication was intercepted, i.e. in transmission or from electronic storage, how long the communication was in storage, whether the communication was received at the recipient or voluntarily conveyed to a 3rd party, and the nature of the information intercepted, i.e. content vs. routing/addressing information. In any memo, brief, or argument these specific factors must be established and then the applicable statutes and case law applied.

However, with the Internet growing in influence and pervasiveness day by day, it is likely that the courts will recognize the need for clarity and, just as they did for the telephone in *Katz,* and unambiguously establish whether society is willing to accept as reasonable an expectation of privacy in e-mail and Internet communications.

Back to Top