# Fourth Amendment Aspects of Internet Communications and Technology

Dennis Nicewander
Assistant State Attorney
17th Judicial Circuit
Ft. Lauderdale, Florida

The emergence of Internet technology has revolutionized the world of communication and information sharing. Unfortunately, criminals have seized this opportunity to enhance the efficiency and productivity of their criminal pursuits. The task ahead of law enforcement is daunting, to say the least. New forms of technology emerge before we are able to master the old ones. The most significant legal issue to arise in this struggle to make order out of chaos is the application of the Fourth Amendment to these emerging technologies. If our economy is going to continue to grow at the rapid pace promised by Internet technology, we must find a way to balance our citizens' right to privacy with the necessity of establishing law and order in this new frontier. As our culture and legal system suffer the growing pains of radical change, it is responsibility of prosecutors to work together with law enforcement to strike a balance between effective police work and privacy rights afforded by the Fourth Amendment. Understanding the role of "reasonable expectation of privacy" is critical to this role. Since most information placed on the Internet is designed for mass distribution, a reasonable expectation of privacy will not apply in the majority of cases. The purpose of this paper is to provide basic guidance and case law concerning this issue as it relates to some of the most common forms Internet technology. The topics will be divided into the following categories:



## General Privacy Cases

Katz v. U.S., 389 U.S. 347, 88 S.Ct. 507 (1967):

In ruling that an individual has an expectation of privacy in telephone conversations he makes from a public telephone booth, the Court made the following observations:

"What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection… But what he seeks

> to preserve as private, even in an area accessible to the public, may be constitutionally protected."
>
> 'My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable."

Smith v. Maryland, 442 U.S. 735, 99 S.Ct. 2577(1979):

In ruling that installation and use of pen register by telephone company at police request did not constitute "search" within meaning of Fourth Amendment, the Court made the following observations:

> "Petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and even if he did, his expectation was not "legitimate." First, it is doubtful that telephone users in general have any expectation of privacy regarding the numbers they dial, since they typically know that they must convey phone numbers to the telephone company and that the company has facilities for recording this information and does in fact record it for various legitimate business purposes. And petitioner did not demonstrate an expectation of privacy merely by using his home phone rather than some other phone, since his conduct, although perhaps calculated to keep the *contents* of his conversation private, was not calculated to preserve the privacy of the number he dialed. Second, even if petitioner did harbor some subjective expectation of privacy, this expectation was not one that society is prepared to recognize as "reasonable." When petitioner voluntarily conveyed numerical information to the phone company and "exposed" that information to its equipment in the normal course of business, he assumed the risk that the company would reveal the information to the police."
>
> "First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies 'for the purposes of

> checking billing operations, detecting fraud and preventing violations of law.'"

California v. Greenwood, 486 U.S. 35, 108 S.Ct. 1625 (1988):

In ruling that police could search through a person's garbage waiting for trash pick-up, the Court made the following observations:

> "Here, we conclude that respondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection. It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public. See *Krivda*, supra, 5 Cal.3d, at 367, 96 Cal.Rptr., at 69, 486 P.2d, at 1269. Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so. Accordingly, having deposited their garbage "in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it," United States v. Reicherter, 647 F.2d 397, 399 (CA3 1981), respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded.
>
> Furthermore, as we have held, the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public. Hence, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."

Note: This case can be used by analogy to Internet mediums. The fact that it deals with people's trash is ironic.

**Email**:

Overview:

The proper means for obtaining a suspect's email from an Internet Service Provider will usually be covered by the Electronic Communications Privacy Act (ECPA). More often than not, a search warrant will need to be obtained to comply with the mandates of 18 U.S.C. 2703. In spite of the fact that most emails are obtained via procedures dictated by federal code in lieu of traditional Fourth Amendment principles, it is still important to consider basic Fourth Amendment issues when seeking such evidence. For instance, ECPA only covers providers of electronic communication services to the public. When email is sought from employers, private email services, or individuals, Fourth Amendment principles

still apply. The key factor in these cases is the reasonable expectation of privacy of the sender or recipient.

In general, sending email is treated much like writing letters. The sender of the email maintains a reasonable expectation of privacy while the email is in transit, but once it reaches its recipient, the expectation diminishes or is eliminated entirely. Just as law enforcement cannot open your mail without a warrant while it is in transit, they cannot read your email while it is stored on a server pending retrieval.

Cases:

U.S. v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996): (***service provider)***

Under circumstances, accused had reasonable, albeit limited, expectation of privacy in e-mail messages that he sent and/or received on computer subscription service, for purpose of determining validity of search; service had policy of not reading or disclosing subscribers' e-mail to anyone except authorized users, and it was service's practice to guard those communications and disclose them to third parties only if given court order.

Implicit promises or contractual guarantees of privacy by commercial entities do not guaranty constitutional expectation of privacy for purpose of determining validity of search.

Fourth Amendment requires that police agencies establish probable cause to enter into personal and private computer, but when individual sends or mails letters, messages, or other information on computer, individual's expectation of privacy diminishes incrementally, and the more open the method of transmission, the less privacy one can reasonably expect, for purpose of determining validity of search.

If sender of first-class mail seals envelope and addresses it to another person, sender can reasonably expect contents to remain private and free from eyes of police absent search warrant founded upon probable cause, but once letter is received and opened, destiny of letter then lies in control of recipient of letter, not sender, absent some legal privilege.

Transmitter of e-mail message enjoys reasonable expectation that police officials will not intercept transmission without probable cause and search warrant, but once transmissions are received by another person, transmitter no longer controls its destiny.

Any of material or information seized and turned over to police agencies by subscriber to computer subscription service, who claimed that child

pornography was being distributed on service, could be introduced into evidence and used in procuring search warrant, but once government wanted to search subscription service's computer files further based upon those chance scraps of information, warrant was required.

For purposes of Fourth Amendment's search and seizure protections, expectations of privacy in e-mail transmissions depend in large part on type of e-mail involved and intended recipient; messages sent to public at large in "chat room" or e-mail that is forwarded from correspondent to correspondent lose any semblance of privacy.

Once e-mail transmissions are sent out to more and more subscribers to computer subscription service, subsequent expectation of privacy incrementally diminishes, though this loss only goes to those specific pieces of mail for which privacy interests were lessened and ultimately abandoned.

"Expectations of privacy in e-mail transmissions depend in large part on the type of e-mail involved and the intended recipient. Messages sent to the public at large in the "chat room" or e-mail that is "forwarded" from correspondent to correspondent lose any semblance of privacy. Once these transmissions are sent out to more and more subscribers, the subsequent expectation of privacy incrementally diminishes. This loss of an expectation of privacy, however, only goes to these specific pieces of mail for which privacy interests were lessened and ultimately abandoned. Thus, any of the material or information seized and turned over to the FBI or to other police agencies by Mr. Dietz was "fair game" for introduction into evidence and for use in procuring a search warrant. However, once the Government wanted to search the computer files further based upon these chance scraps of information, a warrant was required."

U.S. v. Monroe, 52 M.J. 326 (C.A.A.F. 2000): (***employer)***

The transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant, but once the transmissions are received by another person, the transmitter no longer controls its destiny.

Accused had no reasonable expectation of privacy in his e-mail messages or e-mail box in an electronic mail host (EMH) residing on a computer owned by the Air Force, at least from the personnel charged with maintaining the EMH system, where users received specific notice that "users logging on to this system consent to monitoring," and thus it was not a "search" cognizable under the Fourth Amendment when such maintenance personnel opened accused's e-mail messages and subsequently opened his e-mail box while investigating a problem with the system.

U.S. v. Simons, 206 F.3d 392 (4th Cir. 2000): (***employer)***

> Public employer's remote, warrantless searches of employee's office computer did not violate his Fourth Amendment rights because, in light of employer's Internet policy, employee lacked a legitimate expectation of privacy in files downloaded from the Internet; Internet policy clearly stated that employer would "audit, inspect, and/or monitor" employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, "as deemed appropriate," and this policy placed employees on notice that they could not reasonably expect that their Internet activity would be private.

U.S. v. Lifshitz, 369 F.3d 173 (2nd Cir. 2004): (***probation search***)

> "Individuals generally possess a reasonable expectation of privacy in their home computers...They may not, however, enjoy such an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient."

Guest v. Leis, 255 F.3d 325 (6th Cir. 2001): (***computer bulletin board service)***

> "They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose "expectation of privacy ordinarily terminates upon delivery" of the letter."

U.S. v. Charbonneau, 979 F.Supp. 1177 (S.D. Ohio 1997): ***(chat room-detective)***

> "This Court finds that Defendant possessed a limited reasonable expectation of privacy in the e-mail messages he sent and/or received on AOL… E-mail is almost equivalent to sending a letter via the mails. When an individual sends or mails letters, messages, or other information on the computer, that Fourth Amendment expectation of privacy diminishes incrementally… Furthermore, the openness of the "chat room" diminishes Defendant's reasonable expectation of privacy."
>
> "Thus an e-mail message, like a letter, cannot be afforded a reasonable expectation of privacy once that message is received… Moreover, a sender of e-mail runs the risk that he is sending the message to an undercover agent."
>
> "The expectations of privacy in e-mail transmissions depend in large part on both the type of e-mail sent and recipient of the e-mail. See Maxwell, 45 M.J. at 419. E-mail messages sent to an addressee who later forwards the e-mail to a third party do not enjoy the same reasonable expectations of privacy once they have been forwarded."

State v. Evers, 175 N.J. 355, 815 A.2d 432 (N.J. 2003): ***(undercover detective)***

"Defendant clearly had no reasonable expectation of privacy in the content of e-mail he forwarded to fifty-one intended recipients, one of whom happened to be an undercover police officer. Defendant transmitted the forbidden e-mail at peril that one of the recipients would disclose his wrongdoing. There is no constitutional protection for misplaced confidence or bad judgment when committing a crime."

Electronic Communications Privacy Act of 1986 (ECPA), requiring a government entity seeking to procure subscriber information from an Internet service provider to do so by warrant, court order, subpoena, or consent of subscriber, does not afford an objectively reasonable expectation of privacy under the Fourth Amendment.

Assuming California police officer violated Electronic Communications Privacy Act of 1986 (ECPA) and California law by obtaining, from Internet service provider in Virginia, account information for Internet user in New Jersey, exclusionary rule did not apply in prosecution of Internet user in New Jersey for multiple violations of child endangerment statute relating to possession and transmission of child pornography on the Internet, where New Jersey had no control or authority over California police officer, no New Jersey official engaged or participated in any unlawful conduct, and suppressing evidence voluntarily given by Internet service provider to California law enforcement authorities would further no deterrent purpose under New Jersey law.

## Chatrooms

Overview:

The term chatroom typically carries two meanings. A true chatroom is a public forum where individuals discuss topics so that the discussion can be seen by everybody in the room. When individuals meet in a public chatroom they have the option to engage in private instant messages. There are virtually no expectations of privacy in the true chatroom, but privacy interests may arise in the instant message forum. Since instant messaging involves private one-on-one communications, law enforcement cannot intercept the communications without a Title III order. About the only time an issue arises in this context is when an undercover police officer communicates with a suspect via instant messaging under a false identity. In general this does not present a problem in that the suspect is assuming the risk that he that his chat partner is not who he says he is. A problem may arise, however, if the officer assumes the identity of a known acquaintance of the suspect in order to trick him into revealing incriminating

details. This does not appear to be a problem if the acquaintance consents to this interception, but may be a problem if he does not. Special care should also be taken to comply with state laws regarding the interception of communications. Problems occasionally arise when state law does not allow an officer to record conversations with a non-consenting suspect without a court order.

U.S. v. Charbonneau, 979 F.Supp. 1177 (S.D. Ohio 1997):

> "Clearly, when Defendant engaged in chat room conversations, he ran the risk of speaking to an undercover agent. Furthermore, Defendant could not have a reasonable expectation of privacy in the chat rooms. Accordingly, the e-mail sent by Defendant to others in a "chat room" is not afforded any semblance of privacy; the government may present the evidence at trial. In addition, all e-mail sent or forwarded to the undercover agents is not protected by the Fourth Amendment."

U.S. v. Geibel, 369 F.3d 682 (2nd Cir. 2004):

> This case does not involve a Fourth Amendment Issue, but is contains an interesting discussion of expectations of privacy in private chatrooms. The case involves an insider trader conspiracy.
>
> "Although Freeman disclosed the confidential information over the Internet, this does not mean that he had no expectation of privacy. To the contrary, the trio's communications over the Internet were concealed and surreptitious. Freeman used an AOL chatroom named the "YAK chatroom" to tip Cooper and Eskrine. In order for other AOL users to access this chatroom, they would need to know the chatroom's specific name, which was only known to the trio. To further avoid detection, the trio changed chatrooms twice and eventually began communicating through instant messaging. Further, they often coded their communications. Indeed, exclusivity was such a premium that Cooper at one point told Freeman that he wanted Erskine out of the scheme because he felt that Erskine was "telling people about this information." As these measures make clear, the scope of the conspiratorial agreement between Freeman and Cooper was narrow and did not encompass disclosure of inside information to unknown remote tippees such as Conner, Allen, and Geibel."

U.S. v. Meek, 366 F.3d 705 (9th Cir. 2004)

> Police detective's interception of instant messages transmitted over the internet by defendant to minor victim was valid, based upon unilateral consent provided by minor and his father, where minor and his father provided his internet password to detective for purpose of investigating cases of sexual abuse before messages in question were sent.

> Like private telephone conversations, either party to an internet chat room exchange has the power to surrender the other's privacy interest to a third party, so that either party may give effective consent to search the messages.

State v. Turner, 156 Ohio App.3d 177, 805 N.E.2d 124 (Ohio App. 2 Dist.,2004)

> Defendant did not have a reasonable expectation of privacy during exchange or emails and instant messages on the internet, and thus police were not required to obtain a wiretap, in prosecution for attempting to commit unlawful sexual conduct with a minor, importuning, and possession of criminal tools based on defendant soliciting sexual conduct with a minor over the internet; police officer was a part of the instant messages with defendant since officer posed as a minor boy, and defendant's conversations over the internet were not to a known acquaintance.

State v. Moller, 2002 WL 628634 (Ohio App. 2 Dist. 2002): (*Not Reported in N.E.2d*)

> "Moller assumed the risk of speaking to an undercover agent when he engaged in inappropriate chat room conversations and e-mail with a person he believed to be a minor looking for sex with an older man. He took the risk that the "girl" he thought he was speaking to was not who she said she was, and, unfortunately for him, that risk materialized. This does not mean these statements are protected by the Fourth Amendment."
>
> "Like *Hoffa*, Moller took the risk that the 14 year old he thought he was talking to, and planning to engage in sex with, was not who she seemed to be, but was in reality a police officer. This is a risk that anyone visiting a chat room necessarily takes when communicating with strangers. It is easy for anyone using the Internet to adopt a false persona, whether for purposes of law enforcement, or for other and nefarious purposes. It was unreasonable for Moller to assume that his unsuitable conversations would be kept private. Thus, in our view, his statements made in the chat room to a stranger are not entitled to protection under the Fourth Amendment."
>
> "Our opinion does not address what objectively reasonable expectations of privacy an individual might have in circumstances significantly different from those presented in the case before us. Query, for example, an expectation of privacy in a conversation that one reasonably believes one is having with a known acquaintance, perhaps using password, or even encryption, technology, where police officers have defeated the precautions used to protect the communication, and are posing as the known acquaintance."

Commonwealth v. Proetto, 771 A.2d 823 (Pa Super. Ct. 2001):

Defendant did not have a legitimate expectation of privacy in e-mail and chat-room communications with detective, who posed as 15 year old girl while communicating with defendant, and thus there was no violation of defendant's constitutional protection from unreasonable searches and seizures in allowing admission of these communications in defendant's trial for solicitation, obscene and other sexual materials and performances, and corruption of minors, where defendant did not know to whom he was speaking in his Internet chat-room conversations.

State v. Townsend, 147 Wash.2d 666, 57 P.3d 255 (Wash. 2002)

Defendant's e-mail messages and real time Internet client-to-client messages with undercover police officer posing as fictitious child were "private" communications, so that under the telecommunications privacy act, defendant's consent to the recording of the messages may have been required; defendant's subjective intent was that his messages were for fictitious child's eyes only, that intent was made manifest by defendant's message not to "tell anyone about us," and the sexual subject-matter of defendant's communications strongly suggested that he intended the communications to be private, though the interception of the messages was a possibility.

The defendant impliedly consented to recording, on computer of undercover police officer posing as fictitious child, of defendant's real time Internet client-to-client messages to fictitious child, and thus, officer's recording of such messages did not violate the telecommunications privacy act; defendant's instant messaging software contained a "privacy policy" with express warnings that some versions of such software allowed parties to record the content of real time sessions and that the default in some versions was set for recording, and the fact the defendant encouraged the fictitious child to set up an instant messaging account strongly suggested defendant was familiar with the technology.

## Peer-to-Peer

Overview:

"Peer-to-peer" typically refers to file sharing programs on the Internet such as Limewire, KaZaa, eDonkey, Morpheus, iMesh, Grokster and others. Internet users use this technology to share everything from music and videos to child pornography. The reason it is called "peer-to-peer" is because once you find a desired file on the network, a direct connection is established between you and the possessor of the file and the file is transferred directly to your computer. Both law enforcement and the music industry have devised methods of capturing the Internet Protocol address established in this direct connection. Based upon this information, a subpoena can be issued to the Internet Service Provider to establish

the identity of the suspect. Expectations of privacy are rare when using this technology because the user of the program designates a folder on his computer to contain his "shared" files, which are freely available to everybody else on the network. Most privacy issues concerning this technology have been addressed in civil suits brought by the music industry against file sharers. The challenges in this arena are directed at whether the subscriber to an internet service has an expectation of privacy in his identity and whether the industry can obtain that identity via subpoena. Another issue to consider is the emergence of private peer-to-peer networks where only authorized individuals can partake in the file-sharing experience. These private networks may not satisfy the general public's desire for vast amounts of available information, but they may develop popularity within smaller groups such as child pornography collectors.

U.S. v. Ahrndt, (District Court Oregon 2010):

"The issue in this case is whether the Fourth Amendment provides a reasonable, subjective expectation of privacy in the contents of a shared iTunes library on a personal computer connected to an unsecured home wireless network."

The court ruled no expectation of privacy. The opinion contains good language concerning diminished expectation of privacy in unsecured wireless connections.

U.S. v. Stults, F.3d (8th Cir. 2009):

Defendant lacked a reasonable expectation of privacy in files on his personal computer which were accessible to others for file sharing based on his installation and use of **peer**-to-**peer** file sharing software, and thus federal agent's use of file-sharing program to access child pornography files on defendant's computer did not violate defendant's Fourth Amendment rights; even if defendant did not know that others would be able to access files stored on his own computer, defendant knew he had file-sharing software on his computer.

Affidavit in support of search warrant was supported by probable cause; information in affidavit showed that through **peer**-to-**peer** file-sharing program federal agent was able to access and download files directly from defendant's computer that contained child pornography images, and as a result, there was a fair probability that contraband would be found at defendant's residence in his personal computer.

"We hold that Stults had no reasonable expectation of privacy in files that the FBI retrieved from his personal computer where Stults admittedly installed and used LimeWire to make his files accessible to others for file sharing. One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking. As a result, "[a]lthough as

> a general matter an individual has an objectively reasonable expectation of privacy in his personal computer, we fail to see how this expectation can survive [Stults's] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program." Ganoe, 538 F.3d at 1127 (internal citation omitted). Even if we assumed that Stults "did not know that others would be able to access files stored on his own computer," Stults did know that "he had file-sharing software on his computer; indeed, he admitted that he used it-he says to get music [and to download pornography]." Id. As a result, Stults "opened up his download folder to the world, including Agent [Cecchini]." Id. "Having failed to demonstrate an expectation of privacy that society is prepared to accept as reasonable, [Stults] cannot invoke the protections of the Fourth Amendment."

U.S. v. Ganoe, 538 F.3d 1117 (9th Cir. 2008)

> The defendant lacked a reasonable expectation of privacy in the downloaded files stored on his computer, and thus, agent's use of file-sharing software program to access child pornography files on the computer did not violate defendant's Fourth Amendment rights; defendant had installed and used file-sharing software, thereby opening his computer to anyone else with the same freely available program, and defendant had been explicitly warned before completing the installation that the folder into which files were downloaded would be shared with other users in the peer-to-peer network.

Recording Industry Association of America v. Verizon Internet Services, 257 F.Supp.2d 244 (D.D.C. 2003) (Challenge to subpoena powers) (Kazaa)

> "And if an individual subscriber opens his computer to permit others, through peer-to-peer file sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world."

U.S. v. Kennedy, 81 F.Supp.2d 1103 (D.Kan. 2000):

> "On the contrary, the evidence is that defendant's computer had its sharing mechanism turned on. The only reasonable inference is that defendant had done so."
>
> "[W]hat a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection."
>
> Note: This case concerns the privacy of subscriber information, but the language should be applicable to peer-to-peer investigations. The instant case involves a

subscriber who activated file and print sharing, thereby allowing others to access his computer via his IP address. This is similar to the technology utilized by peer-to-peer technologies, like Kazaa.

Elektra Entertainment Group, Inc., v. Does 1-9, 2004 WL 2095581 (S.D.N.Y. 2004)

"Finally, Doe No. 7 is entitled to only a minimal "expectation of privacy in downloading and distributing copyrighted songs without permission." Id. (citing *Verizon*, 257 F.Supp.2d at 260-61, 267-68). NYU's privacy guidelines state that it will comply with a civil subpoena seeking identifying information without a student's consent provided that the student is first notified of the request. And NYU's Network Responsibilities state that users must obtain the permission of copyright owners before copying protected material."

Note: This case involves users of KaZaa attempting to quash subpoenas by the music industry to reveal their identities. The subpoenas were issued to the university where the students attended.

State v. Thornton, Slip Copy, 2009 WL 3090409 (Ohio App. 10 Dist.), 2009 -Ohio-5125

The Fourth Amendment to the United States Constitution prohibits unreasonable searches and seizures. A search occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. State v. Keith, 10th Dist. No. 08AP-28, 2008-Ohio-6122, ¶ 16, quoting United States v. Jacobsen (1984), 466 U.S. 112, 113, 104 S.Ct. 1652, 1656. An individual cannot be said to have a reasonable expectation of privacy in that which he knowingly exposes to the public. State v.. Lopez (Sept. 28, 1994), 2d Dist. No. 94-CA-21, citing Katz v. United States (1967), 389 U.S. 347, 351, 88 S.Ct. 507, 511; Keith.

Appellant knowingly exposed to the public the files found on Perry's computer and the IP address associated with that computer through the use of the Limewire program on the computer. Therefore, he had no reasonable expectation of privacy in that evidence. United States v. Ganoe (C.A.9, 2008), 538 F.3d 1117, 1127 (no legitimate expectation of privacy in files defendant made available to public using Limewire software); United States v. Borowy (D.Nev.2008), 577 F.Supp.2d 1133, 1136 (same); United States v. Forrester (C.A.9, 2008), 512 F.3d 500, 510 (no reasonable expectation of privacy in IP address); United States v. Li (Mar. 20, 2008), S.D. Cal. No. 07 CR 2915 JM, at 5, slip opinion (same). In that situation, Fourth Amendment protections are not implicated because a search does not occur. See Keith, citing State v. Sheppard (2001), 144 Ohio App.3d 135, 141.

**Internet Provider Subscriber Records**

Overview:

Case law is clear that subscribers to Internet service providers do not have a reasonable expectation in their basic subscriber information. They may have a reasonable expectation in the content of their communications, but not their basic identity information.

U.S. v. Christie, --- F.3d ----, 2010 WL 4026817 (C.A.3 (N.J.))

User of internet website that contained child pornography had no reasonable expectation of privacy, of kind protected by the Fourth Amendment, in identifying address information that his internet service provider had assigned to his home computer.

U.S. v. Beckett, Slip Copy, 2010 WL 776049 C.A.11 (Fla.),2010.

Defendant did not have reasonable expectation of privacy in subscriber identification information given to internet services providers (ISP) and telephone companies, within scope of Fourth Amendment; investigators did not recover any information related to content, but instead, received identifying information transmitted during internet usage and telephone calls necessary for ISPs and telephone company to perform their services.

U.S. v. Bynum, --- F.3d ----, 2010 WL 1817763 (C.A.4 (N.C.))

Defendant did not have a subjective expectation of privacy in his subscriber information, as required to possess a legitimate privacy interest for purposes of his prosecution for transporting and possessing child pornography, where he voluntarily conveyed his name, email address, telephone number and physical address to his internet and phone companies, deliberately chose a screen name derived from his first name, and voluntarily posted his photo, location, sex and age on his profile page.

U.S. v. Perrine, 518 F.3d 1196 (10th Cir. 2008):

Defendant had no expectation of privacy, under Fourth Amendment, in government's acquisition of his subscriber information, including internet protocol (IP) address and name, from third-party service providers, pursuant to Electronic Communications Privacy Act (ECPA) and Pennsylvania law, authorizing such disclosure upon specific and articulable facts showing reasonable grounds to believe records were relevant and material to ongoing criminal investigation, as would support issuing search warrant that resulted in seizure of defendant's computer with thousands of images of child pornography; where defendant voluntarily transmitted such information to internet providers and enabled peer-

to-peer file sharing on computer, which allowed anyone with internet access ability to enter his computer and access certain folders.

U.S. v. Forrester, 495 F.3d. 1041 (9th Cir. 2007):

Use of computer surveillance techniques that revealed the to and from addresses of e-mail messages, the addresses of websites visited by defendant, and the total amount of data transmitted to or from defendant's internet account did not amount to a "search" in violation of the Fourth Amendment; e-mail and internet users had no expectation of privacy in the addresses of their e-mail messages or the addresses of the websites they visited, because they should know that such information was sent and accessed through their internet service provider and other third parties, and the addresses did not reveal the contents of communications.

Even if government's use of computer surveillance techniques to obtain to and from addresses for e-mail messages and the addresses of websites visited by the defendant was beyond the scope of the pen register statute, suppression of the evidence the government obtained through such surveillance was not available as remedy, in prosecution for conspiracy to manufacture ecstasy and related offenses, absent showing that the surveillance violated the law, or that suppression was remedy set forth in the pen register statute.

U.S. v. Kennedy, 81 F.Supp.2d 1103 (D.Kan. 2000):

Defendant did not have a Fourth Amendment privacy interest in his Internet subscriber information; when defendant entered into an agreement with provider for Internet service, he knowing revealed all information connected to his subscriber address.

U.S. v. Hambrick, 225 F.3d 656 (4th Cir. 2000): *unpublished*

"The ECPA does not represent a legislative determination of a reasonable expectation of privacy in non-content information released by ISPs."

"The information the government received from MindSpring consisted of Hambrick's subscriber information, which included his name; billing address; home, work, and fax phone numbers; and other billing information."

"While under certain circumstances, a person may have an expectation of privacy in content information, a person does not have an interest in the account information given to the ISP in order to establish the e-mail account, which is non-content information."

"Disclosure of this non-content information to a third party destroys the privacy expectation that might have existed previously. In this case, the government never utilized the non-content information retrieved from MindSpring to attain additional content information, such as the substance of Hambrick's e-mails. In this case, as in *Miller,* there is no legitimate expectation of privacy in information "voluntarily conveyed to [a third party] and exposed to their employees in the ordinary course of business." Miller, 425 U.S. at 442."

"The invalidity of the subpoena in this case does not trigger the application of the Fourth Amendment, as Hambrick had no privacy interest in the non-content information obtained as a result of the subpoena."

Note: This case contains a good discussion of federal precedent concerning expectations of privacy.

U.S. v. Cox, 190 F.Supp.2d 330 (N.D.N.Y.,2002)

Criminal defendant had no Fourth Amendment privacy interest in subscriber information given to his Internet service provider.

**Websites:**

Overview: Courts have generally ruled that there is no reasonable expectation of privacy on information placed on web sites. However, the courts have alluded to the fact that a reasonable expectation may exist of measures are taken to protect that information, such as passwords.

United States v D'Andrea, F.Supp.2d (D.Mass. 2007)

For Fourth Amendment purposes, there can be no reasonable expectation of privacy in matters voluntarily disclosed or entrusted to third parties, even those disclosed to person with whom one has confidential business relationship.

Internet users have no reasonable expectation of privacy protected by Fourth Amendment in their subscriber information, length of their stored files, and other noncontent data to which service providers must have access.

State child protection official did not violate defendants' Fourth Amendment rights by accessing password-protected website and downloading images of defendants sexually abusing young child, where official received log-in name and password for website from anonymous caller, and caller was not acting as state's agent in reporting abuse.

*At day's end, this case falls clearly into the "assumption of the risk" exception identified in Warshak and Supreme Court precedent.FN17 "It is well-settled*

> *that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information." Jacobsen, 466 U.S. at 117. See also United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F.1996) (the sender of an email runs the risk that its recipient will publish its contents). Thus, even granting defendants a reasonable expectation of privacy in the graphic website images of Jane Doe, by sharing the website access information with the anonymous caller, defendants took the risk that their right to privacy in the website's contents could be compromised.*

U.S. v. Gines-Perez, 214 F.Supp.2d 205 (D.Puerto Rico,2002)

As a matter of first impression, use of a picture of a store's employees, downloaded from store's website by a government agent, to identify defendant did not violate his privacy rights, even though website was allegedly private and under construction at time picture was downloaded; defendant had no subjective expectation of privacy in photograph placed on the public medium of the internet, society was not prepared to recognize as reasonable any expectation of privacy in information placed on internet, and picture was obviously placed on website for commercial purposes.

"The Court is convinced that placing information on the information superhighway necessarily makes said matter accessible to the public, no matter how many protectionist measures may be taken, or even when a web page is "under construction." While it is true that there is no case law on point regarding this issue, it strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, **without taking any measures to protect the information."**

"The defense may claim that the web site in controversy was not intended to be 'public' or 'commercial' in nature. But it is not the intention of the person who uses the Internet to communicate information which is important; it is the medium in which he or she places the information and the nature of the materials placed on the web which are important. A person who places information on the information superhighway clearly subjects said information to being accessed by every conceivable interested party. Simply expressed, if privacy is sought, then public communication mediums such as the Internet are not adequate forums without protective measures."

"A reasonable person cannot place 'private' information--such as a 'private' photograph--on the Internet, if he or she desires to keep such information in actual 'privacy.' A reasonable person does not protect his private pictures by placing them on an Internet site."

> "The Court finds that this society is simply not prepared to recognize as 'reasonable' a claim that a picture on the Internet is 'private' in nature, such that the Government cannot access it. In fact, the Court believes that our society would recognize the opposite; that a person who places a photograph on the Internet precisely intends to forsake and renounce all privacy rights to such imagery, particularly under circumstances such as here, where the Defendant did not employ protective measures or devices that would have controlled access to the Web page or the photograph itself."

J.S. ex rel. H.S. v. Bethlehem Area School Dist. 757 A.2d 412 (Pa.Cmwlth.,2000)

> School district did not violate middle school student's right to privacy when district accessed student's unprotected Internet website that was titled "Teacher Sux" and that contained threatening and disrespectful comments about teacher and principal.
>
> "Likewise, the creator of a web-site controls the site until such time as it is posted on the Internet. Once it is posted, the creator loses control of the web-site's destiny and it may be accessed by anyone on the Internet. Without protecting the web-site, the creator takes the risk of other individuals accessing it once it is posted. Accordingly, we conclude that the trial court was correct in its determination that Student maintained no expectation of privacy in the web-site."

Moreno v. Hanford Sentinel, Inc. ,(Cal.App. 5 Dist.)

> Principal did not violate student's family's privacy by having online journal entry republished in newspaper.
>
> A high school principal did not commit an invasion of privacy by allegedly having a student's sister's disparaging "ode to Coalinga" reprinted and attributed to the sister under her full name in the Letters to the Editor section of Coalinga's newspaper. The sister had posted the Ode in her MySpace online journal on a page that identified her by her first name and photograph, but she removed the Ode after six days, before learning that the principal had given it to the editor of the newspaper. The republication allegedly resulted in death threats and a shot fired at the family home, forcing the family to move. The Court of Appeal explained that no reasonable person would have had an expectation of privacy regarding the published material after it appeared on the MySpace page.

**Bulletin Board**

Guest v. Leis, 255 F.3d 325 (6th Cir. 2001):

"Home owners would of course have a reasonable expectation of privacy in their homes and in their belongings-- including computers--inside the home. Bulletin board users would not share the same interest in someone else's house or computer, so they would not be able to challenge the search of the homes and the seizure of the computers as physical objects. Their interest in the computer content presents a different question and would depend on their expectations of privacy in the materials. In the *O'Brien* case, the SI BBS posted a disclaimer stating that personal communications were not private. This disclaimer defeats claims to an objectively reasonable expectation of privacy for the SI BBS users."

**University Usage Logs**

U.S. v. Butler, 151 F.Supp.2d 82 (D.Maine 2001):

Session logs maintained by university computer lab were maintained for benefit of university, and therefore defendant charged with receiving child pornography over Internet had no expectation of privacy in logs showing when defendant used university computers.

Defendant charged with receiving child pornography over Internet had no reasonable expectation of privacy in hard drives of university computers; defendant pointed to no statements or representations made to him as user of computers, nor to any practices concerning access to and retention of contents of hard drives, not even password requirements, which could have created expectation of privacy.

**Text Messages**

Quon v. Archwireless, 529 F.3d 892 (9th Cir. 2008):

Police officer had reasonable expectation of privacy, under Fourth Amendment, in text messages sent to and from his city-owned pager, even though department's written computer and e-mail policy decreed that no expectation of privacy should attach to use of those resources, and even assuming that messages constituted public records under California Public Records Act (CPRA); police lieutenant in charge of pagers had established informal policy under which officer's messages would not be audited if he paid for usage overages, and CPRA did not diminish officer's reasonable expectation.

Police department's search of content of officers' text messages sent and received via city-owned pagers, which was reasonable at its inception based on noninvestigatory work-related purpose of ensuring that officers were not being required to pay for work-related expenses when they reimbursed city for usage overages, was nevertheless

unreasonable in scope and thus violative of Fourth Amendment; less intrusive means existed to achieve same end, including warning officers that content of messages would be reviewed in future to ensure work-related uses.

Employees of city police department had expectation of privacy, under Fourth Amendment, in content of text messages that they sent and received using city-owned pagers, and that were archived by wireless service provider that contracted with city; fact that provider had capability to access content for its own purposes did not remove that expectation.