2 OKLA. J. L. & TECH. 28 (2005)
www.okjolt.org

Abstract

E. Parker Lowe is a 2004 graduate of the University of Oklahoma College of Law and a 2003-2004 member of the Oklahoma Journal of Law and Technology. Below, Mr. Lowe analyzes the Fourth Amendment implications of electronic mail (email).

Mr. Lowe argues that the principle that the Fourth Amendment protects people and not mere places leads to the conclusion that there is some amount of Fourth Amendment protection applicable to the contents of private emails. Part II of this note provides an overview of Internet technology to provide a framework for analysis. Part III discusses the susceptibility of email to interception which could undermine its protection as private under traditional Fourth Amendment analysis. Part IV includes a discussion of major Fourth Amendment cases and analogies that can be drawn therefrom to the email context. Part V poses the question of whether or not the Electronic Communications Privacy Act of 1986 can serve as a basis for a reasonable expectation of privacy. Mr. Lowe concludes by arguing for the announcement of a rule that sets definite standards for the protection of email users' privacy.

Edited by Jennifer Stevenson

EMAILER BEWARE: THE FOURTH AMENDMENT AND ELECTRONIC MAIL

> "The progress of science in furnishing the Government with means of espionage is not likely to stop...Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[1]
>
> - Olmstead v. U.S., Justice Brandeis (dissenting) -

I. Introduction

The Internet is the phenomenon of our times. It is both a blessing and a curse. It allows us to do so many things in an instant with just the touch of a button, yet it also presents many societal problems. The Internet has revolutionized business and personal communication.[2] Not only are the uses of the Internet incredible, so is its growth. It has been estimated that more than

[1] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).
[2] Robert A. Pikowsky, *Legal and Technological Issues Surrounding Privacy of Attorney Client Communications Via Email*, 43 ADVOCATE 16 (2000).

one billion users will connect to the Internet by the end of 2005.[3] As the Internet continues to expand and becomes an entire branch of society, we must be wary of the many concerns that come along with its use. One must understand the risks of sending and receiving communication via the Internet and how much privacy, if any, is afforded to it in light of the U.S. Constitution. As different technologies emerge, society must decide how much privacy will be given to these new forms of communication. One form of communication that society must learn how to deal with is the one-to-one messaging form known as electronic mail or "email." This note addresses an alarming phenomenon: many email users expect privacy in their messages, but the U.S. Constitution does not seem to reflect this expectation. Federal statutes have been passed recently, such as the U.S.A. Patriot Act,[4] which shows a trend of Americans' privacy shrinking. Thankfully, there is a bottom line of privacy protection that cannot be stripped: the Fourth Amendment. However, according to Fourth Amendment jurisprudence, traditional privacy protections may not apply to email. If the Fourth Amendment does not protect email, then the only national protection that is afforded to email is through federal statutes passed by Congress, which will only further diminish if the trend continues.

Because there are many similarities between email and letters, it can be argued that email should receive the same privacy protection as first class mail. There is a reasonable expectation of privacy in first class mail as annunciated by the Court in *United States v. Jacobsen*.[5] However, the question presented here is whether an email and a first class letter are so similar as to receive the same protection. Both email and letters are written forms of communication,

---

[3] *Worldwide Internet Users Will Top 1 Billion in 2005*, COMPUTER INDUSTRY ALMANAC, INC., Sept. 3, 2004, *available at* http://www.c-i-a.com/pr0904.htm.
[4] Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of U.S.C).
[5] 466 U.S. 109, 114 (1984); Megan Connor Bertron, *Home Is Where Your Modem Is:An Appropriate Application of Search and Seizure Law to Electronic Mail*, 34 AM. CRIM. L. REV. 163, 172 (1996).

usually from one person to another, which can be copied and stored for long periods of time.[6] Email and first class mail allow users to send large amounts of information, including attachments, for a relatively low cost.[7] Moreover, both provide an easy medium for solicited and unsolicited advertisements to specific addresses and persons. However, because of the technology email uses, first class mail and email differ much in their operation. If a first class piece of mail went through the same process as an email does in order to reach its destination, it might look something like this: the sender would drop a first class letter in a mail box; then a postman would shred the letter and take the pieces to the post office for sorting; next, the different pieces of the letter would be sent in separate trucks, possibly through different cities, until they all reached the same destination; upon arrival at its destination, the shredded letter would then piece itself back together in its original form. The destination is not in the recipient's mailbox, as it is with a normal first class letter, but it arrives at a centralized location where the recipient picks up the mail. Furthermore, this process is complete in a matter of seconds. Therefore, this process demonstrates that comparing email to first class mail is not very straight forward.

II. An Internet Overview

Before one can understand the privacy implications email presents, a basic history and understanding of the Internet is appropriate. The Internet is not a physical place, but rather a global interconnected network of computers and hardware, which allows the transmission and reception of information and communication.[8] A network is simply a group of computers linked

---

[6] *Id*. at 182-83.
[7] *Id*.
[8] ACLU v. Reno, 929 F. Supp. 824, 830 (E.D. Pa. 1996).

together that are able to communicate between each other.[9] From its origins as an experimental project in 1969 by the U.S. Department of Defense, the Internet has allowed the transmission of communications almost instantaneously.[10] Originally, the Internet, then known as the ARPANET, connected defense contractors, the military and certain universities in order to establish a form of communication in case of nuclear war.[11] In 1983, the ARPANET was divided into two different systems, one system for the military known as MILNET, and the other system devoted to more research of networking, known as the DARPA Internet.[12] The networking system, DARPA Internet soon became the phenomenon of what is known today simply as the Internet.[13] The Internet now consists of millions of networks, routers, and devices, which send and receive electronic information between each other.[14] The hardware that makes up the Internet is owned and operated by various government institutions, private organizations, businesses, not-for-profit organizations, and private citizens.[15] Similar to its early years as an experiment, the Internet's main use is communication. Roughly six common categories of Internet communication exist:

(1) one-to-one messaging,
(2) one-to-many messaging,
(3) distributed message databases,
(4) real time communication,
(5) real time remote computer utilization, and
(6) remote information retrieval. [16]

---

[9] *Id.* at 831.
[10] *Id.*
[11] Pikowsky, *supra* note 2, at 16.
[12] *Id.*; *Reno*, 929 F. Supp. at 831.
[13] *Reno*, 929 F. Supp. at 831.
[14] Jeff Tyson, *How Internet Infrastructure Works*, HOW STUFF WORKS, *at* http://computer.howstuffworks.com/internet-infrasctructure.htm (last visited Apr. 9, 2004)
[15] *Reno*, 929 F. Supp. at 831.
[16] *Id.* at 834.

One-to-one messaging on the internet consists of electronic mail, or email.[17] When one sends an email, it is impossible to determine the path that message will take to reach the recipient.[18] In fact, an email sent to one person might not take the same path as a different email sent seconds later to the very same person.[19] To complicate things more, the Internet uses an operation known as "packet switching" where an individual message is divided up into smaller chunks known as "packets."[20] Once the email is divided into these packets, it is sent independently through the Internet and later reassembled at its destination.[21] Since the Internet was designed for efficiency of communication during a nuclear war, these packets do not always travel through the same channels, but instead are routed through different networks when it is more efficient.[22] Once an email arrives at its destination, it is not located at the recipient's computer but at the user's email service provider.[23] The email will remain on the email provider's system until the recipient retrieves the message.[24] Once the intended recipient receives the email, the message will usually be downloaded to his hard drive and erased from the email provider's host computer, but this is not always the case.[25] Pursuant to company policies, email providers do not erase the message for a certain period.[26] Finally, other email providers store all of the user's email on its server until deleted by the user. With these types of email

---

[17] *Id.*

[18] *Top 10 Places Your Email Can Be Intercepted*, WILD ID, http://www.wildid.com/email-interception.asp (last visited Mar. 27, 2004) [hereinafter *Top 10*].

[19] *Reno*, 929 F. Supp. at 831.

[20] *Id.* at 832.

[21] *Id.*

[22] *Id.*

[23] Pikowsky, *supra* note 2, at 17.

[24] *Id.*

[25] *Id.*

[26] *Id.*

providers, a user's email is never automatically downloaded to his hard drive, unless he takes independent action.

III. Email Susceptibility

Such a complicated protocol results in the little chunks of one email traveling through an indeterminate amount of systems and networks before reaching the intended recipient.[27] Each time an email travels through a different network, it risks interception by unwanted eyes.[28] As the email travels through cyberspace it is subjected to several million Internet users with the ability and knowledge to intercept that message at numerous points.[29] All Internet traffic that flows to and from a user's computer passes through that user's Internet Service Provider ("ISP"), making this point one of the easiest places to intercept an email or Internet traffic.[30] This is the reason the FBI targets this point in order to implement its Carnivore surveillance technology (which will be discussed further).[31] Many ISPs provide users with email service also, but if one uses an independent email provider, then another point of interception exists: the independent email provider's network.[32] Hackers or renegade employees of the email service can intercept email just as easily when the messages pass through the independent email provider's server as they can when the messages pass through an ISP's server.[33] If a person sends an email from his office computer, the email travels through the corporate network, which makes the message susceptible to interception by co-workers and network administrators.[34] When a person uses a broadband technology such as a cable modem, a shared local loop is used, meaning all

---

[27] *Top 10*, *supra* note 18.
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*

neighborhood Internet traffic shares the same physical wires.[35] With certain bits of hardware and some know-how a hacker can easily intercept an email on its way out of the sender's neighborhood.[36] Finally, as wireless networks become prevalent users should be aware that email traffic is susceptible to interception at the base station for the antenna, which is the point where the email is converted to wire network signals.[37] These examples are by no means the only places email can be compromised and are not even an exhaustive list of the most susceptible places for an email.

Today, renegade hackers are not the only threat to the privacy of email. The federal government also uses at least one hacker technology to intercept email known as a "packet sniffer."[38] Packet sniffers are programs that look at all the information, or packets, that pass over the network to which they are connected.[39] The FBI is currently using its third generation

of online detection systems known as the DragonWare Suite, which allows the FBI to reconstruct emails, downloaded files and web pages.[40] The infamous Carnivore is a part of DragonWare Suite that gathers all information on a network, essentially making it a packet sniffer.[41] With millions of hackers on the Internet and so many points of vulnerability for electronic mail, why should anyone reasonably expect their email to remain private? And if there is no reasonable expectation of privacy and emails are being seen by unwanted eyes already, why should the government be barred from reading your email also?

---

[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Packet Sniffing*, HOW STUFF WORKS, *at* http://computer.howstuffsworks.com/carnivore2.htm (last visited Mar. 4, 2004).
[39] *Id.*
[40] Jeff Tyson, *How Carnivore Works*, HOW STUFF WORKS, *at* http://computer.howstuffworks.com/carnivore1.htm (last visited Mar. 4, 2004). *See also* Scott Griner, *FBI's Carnivore: Under the Fourth Amendment and the USA Patriot Act*, 1 OKLA. J.L. & TECH. 2 (2003), *available at* http://www.okjolt.org/published/2003okjoltrev2.cfm.
[41] *Id.*

IV. Constitutional Protection?

The Fourth Amendment guarantees "[t]he right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[42] A search or seizure can only occur if a legitimate expectation of privacy exists.[43] Therefore, this section will address whether it is objectively reasonable for a person who sends or receives an email via the Internet to legitimately expect the message to remain private. Many standards of protection might be applied to email, but it is unclear as to which one should be applied. It is important to look to applicable Fourth Amendment jurisprudence to determine if the present case law can logically be applied or if another standard needs to be crafted for this ever changing technology.

A. *Katz v. United States*

1. Facts

In *Katz v. United States*,[44] the petitioner was charged and convicted of transmitting wagering information by telephone in violation of a federal statute.[45] Without judicial authorization, FBI agents attached an electronic device outside of a public telephone booth, which allowed the agents to listen and record the calls the petitioner made inside the phone booth.[46] The evidence obtained through the electronic device was used at trial to convict the petitioner.[47] The petitioner claimed that the evidence had been obtained in violation of the Fourth Amendment, but the court of appeals affirmed the conviction and rejected the claim since there had been no physical intrusion of the telephone booth.[48] The Supreme Court then granted

---

[42] U.S. CONST. amend. IV.
[43] United States v. Jacobsen, 466 U.S. 109, 113 (1984).
[44] 389 U.S. 347 (1967).
[45] *Id.* at 348.
[46] *Id.*
[47] *Id.*
[48] *Id.* at 348-49.

certiorari to consider whether the petitioner had a legitimate expectation of privacy in his telephone conversation which took place inside a closed phone booth.[49]

2. Majority Opinion

The Supreme Court had previously relied on the "trespass" doctrine of *Olmstead v. United States*[50] and *Goldman v. United States*,[51] which said a search and seizure could not occur unless a physical trespass had taken place, but the Court overturned this narrow policy holding that people, and not merely areas, are protected by the Fourth Amendment.[52] Accordingly, the Court said the fact the electronic device used was not inside the phone booth was not significant to the constitutional inquiry.[53] The Court concluded because the petitioner justifiably relied upon the phone booth to be private, by electronically listening and recording the petitioner's words, the Government had performed a search and seizure within the meaning of the Fourth Amendment. Consequently Petitioner's Fourth Amendment privacy interest had been violated.[54]

3. Concurring Opinion

Justice Harlan's famous articulation of the present day test for whether if a Fourth Amendment search has occurred set forth a two-fold inquiry: (a) has the person exhibited an actual, or a subjective expectation of privacy and (b) is that expectation one that society is prepared to recognize as reasonable?[55] In the case at bar, the exhibition of an actual expectation was seen by the petitioner occupying the phone booth, closing the door, and paying the toll.[56]

---

[49] *Id.* at 349.

[50] 277 U.S. 438, 466 (1928).

[51] 316 U.S. 129 (1942).

[52] *Katz*, 389 U.S. at 353.

[53] *Id.*

[54] *Id.*

[55] *Id.* at 361 (Harlan, J., concurring).

[56] *Id.* (Harlan, J., concurring).

Justice Harlan then said, as the Court found in *Rios v. United States*,[57] society has recognized the expectation of privacy of a phone booth as reasonable.[58]

4. *Katz*'s Analysis of Email

The Court in *Katz* could not have foreseen this test might be applied to modern privacy concerns with email. Very few courts have decided how much protection an email deserves, and none have specifically decided what privacy rights exist for email in transit. However, courts have reasoned that Fourth Amendment protection diminishes when sending mail or other information by a computer.[59] But the extent of the diminution is unclear. Therefore, it is helpful first to apply the two part test of *Katz*. To meet the first prong of *Katz*, the existence of a subjective expectation, one can argue that by using electronic mail to communicate in the first place, the user exhibits an expectation that the message will remain private because most email users do not know how susceptible email is to interception. Courts may find this is enough for the subjective prong, especially today because email is such a new form of communication and is not understood very well. This argument is strengthened when a person takes extra steps to ensure privacy in his email by using an email provider that requires a username and password to send and receive messages, or using encryption technology to encode messages as it travels over the Internet. Courts might also find a subjective expectation for one-to-one email messaging simply because it is directed and addressed to only one party. However, if that same email is sent to other recipients, forwarded, or the sender uses a more open method of sending the message via the Internet (such as a public chat room), a court will likely see this as voluntarily

---

[57] 364 U.S. 253 (1960).
[58] *Katz*, 389 U.S. at 361.
[59] United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997); United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996).

exposing the message to a third party, thus eliminating the expectation of privacy.[60] The second element of *Katz*, whether there is an objectively reasonable expectation in an email, will likely depend on many factors such as the type of Internet communication that is used, the recipient of the message, and the relationship between the user and email provider.[61] The Sixth Circuit has held that users of a computer bulletin board do not have a legitimate expectation of privacy because this is a public posting of information.[62] The court in *United States. v. Maxwell*[63] held that there is no reasonable expectation in emails sent to chat rooms with several members.[64] Courts have also held that there is no reasonable expectation of privacy in email conversations made in a private, one-on-one chat room.[65] Further, if an employee uses his employer's email system, then the expectation of privacy decreases and might not exist at all no matter what form of electronic communication is used. In *United States v. Monroe,*[66] the court held that a member of the U.S. Air Force had no legitimate expectation of privacy in his email messages when government personnel were responsible for maintaining the system which might require monitoring email. In *Monroe*, the court considered other factors such as the email host system used to send and receive emails was owned by the government, and all users were warned of possible monitoring by government employees once logged in to their email accounts.[67] The court in *Smyth v. Pillsbury Co*.[68] affirmed an employee being fired for comments made over the company's email network in holding there was no reasonable expectation of privacy in email if

---

[60] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[61] *Maxwell*, 45 M.J. at 419.
[62] Guest v. Leis, 255 F.3d 325, 332 (6th Cir. 2001).
[63] 45 M.J. 406 (C.A.A.F. 1996).
[64] *Id.* at 419.
[65] United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997); Commonwealth v. Proetto, 771 A.2d 823 (Pa. Super. 2001).
[66] 52 M.J. 326 (C.A.A.F. 2000).
[67] *Id.* at 330.
[68] 914 F. Supp. 97 (E.D. Pa. 1996).

the message was sent to a supervisor voluntarily, despite assurance by the company that all email would remain private and would not be used as grounds for termination.[69] The court in *McLaren v. Microsoft Corp.*[70] held there is no reasonable expectation of privacy in email when the messages are sent and received over the employer's email system and are stored on the employee's office computer.[71] The *McLaren* court reasoned that a computer is provided not for storage of personal property, but rather for work functions, and that the email stored on the employer's computer is "merely an inherent part of the office environment."[72] Therefore, it seems courts will only find a reasonable expectation of privacy in email in very fact-specific circumstances, if any at all. A reasonable expectation of privacy might exist if a person sends an email message to one recipient using a home computer that is connected to a network that does not monitor email, and the message is not sent to any other party other than the intended original recipient. One must consider whether, if federal statutes that give some protection to electronic communications, such as the Electronic Communications Privacy Act ("ECPA"), were not in place, the Fourth Amendment would extend to protect email from the government's eyes at all. Therefore, it is helpful to look to more recent Supreme Court cases to determine the Constitutional protection of email.

B. *California v. Greenwood*[73]

1. Facts

Without a warrant, on April 6, 1984, in connection with an investigation of possible narcotics trafficking, an investigator of the Laguna Beach Police Department asked the neighborhood trash collector to pick up the plastic garbage that had been left by the respondent

[69] *Id.* at 101.
[70] No. 05-97-00824-CV, 1999 WL 339015 (Tex. App. 1999).
[71] *Id.* at 4.
[72] *Id.*
[73] 486 U.S. 35 (1988).

on the curb in front of his house.[74] The trash collector complied and the officer searched through the trash and found evidence of narcotics use.[75] The officer then obtained a warrant to search the respondent's home as a result of the evidence found in the trash bags. After finding more incriminating evidence at the respondent's home, the respondent was arrested on federal narcotics charges.[76] After posting bond, police officers suspected continued drug trafficking, so they intercepted the respondent's garbage bags again from the neighborhood trash collector without judicial authorization.[77] The second search of the respondent's trash bags resulted in another search warrant for his house, which produced even more evidence of narcotics trafficking, led to the respondent's second arrest.[78] The superior court held that warrantless "trash searches violate the Fourth Amendment and the California Constitution."[79]

The California appellate court affirmed the decision.[80] The U.S. Supreme Court granted certiorari to determine whether warrantless searches and seizures of garbage bags left on the curb outside of a house violated the Fourth Amendment.

2. Majority Opinion

The Court applied the *Katz* two-prong test to determine if there was search of the garbage bags for purposes of the Fourth Amendment.[81] The Court found the respondent might have exhibited an expectation of privacy by placing the trash in an opaque bag for a limited time on the curb; however, society must accept this expectation as objectively reasonable for the

---

[74] *Id.* at 37.
[75] *Id.* at 37-38.

[76] *Id.* at 38.
[77] *Id.*
[78] *Id.*
[79] *Id.* at 37.
[80] *Id.*
[81] *Id.* at 39.

expectation to exist.[82] The Court found that society did not exhibit such an expectation.[83] It reasoned that because the garbage bags were exposed to the public and were readily accessible to animals, children, snoops, and others within the general public, Fourth Amendment protection did not protect the bags.[84] Further, police should not be expected to turn away from evidence of criminal activity that could have been observed by any member of the public.[85]

3. Email and *Greenwood*

After seeing the alarming number of hackers, the numerous points of weakness in emails, and the technologies used to aid in hacking, it is possible that use of the Internet to communicate can result in exposure of email messages to the general public. Because the Court held that exposing property to the public results in a lose of Fourth Amendment protection,[86] courts may find sending electronic mail via the Internet analogous to placing garbage bags in front of the home, thus a reasonable expectation of privacy as to emails will not exist.

If any Internet user types 'how to hack' or 'packet sniffer' on a search engine, thousands of links will come up ready to sell any Internet user email surveillance technology. The *Greenwood* Court would likely find that children, snoops, and others within the general public could easily seize another's email with no more effort than taking someone's garbage bag and rummaging through the contents. Therefore, treating email in cyberspace as garbage bags on the curb is not as far fetched as it might sound. However, the Court in *Greenwood* never defined what constitutes the "public." Even if it had, the definition of "public" for garbage bags might be different than the definition of "public" for the electronic mail. The "public" for email

---

[82] *Id.* at 40.
[83] *Id.*
[84] *Id.*
[85] *Id.* at 41.
[86] *Id.* at 40.

purposes could be the American population, the world population, the American Internet population, or the world Internet population. This determination could have an affect on Fourth Amendment protection of email. If "public" is defined as the American Internet population or the world Internet population, then it will be more likely that sending an email means exposing the message to the public because, as discussed above, most Internet users can download software to intercept email fairly easily. If "public" is defined as the American population or the world population in general, there might not be enough Internet users today to suggest that email in cyberspace is exposed to the public, but rather a smaller branch of society. At some point in the future, however, enough Americans and world citizens will be Internet users that using the Internet will be considered the "public." At that point, sending email via the Internet will be considered exposing it to public eyes and, consequently, losing its reasonable expectation of privacy. However, encryption technology, if it is used, would negate this analogy. But what happens when hacker technology is able to defeat encryption technology?

The Court in *Greenwood* also held that there was no reasonable expectation of privacy because the respondent had conveyed the garbage bag to a third party.[87] If a court finds this reasoning to be applicable to an email, the question becomes: does an email sender knowingly convey his message to a third party by using the Internet? Few Internet users are *unaware* of the possibility of being hacked while online; likewise, few contemplate the ease with which this can be accomplished. Therefore, perhaps for a few, ignorance is bliss and the Fourth Amendment protects them, but it is unlikely any court would want to encourage ignorance. As more hacker attacks occur and more federal software such as Carnivore comes to national attention, email might then lose its reasonable expectation of privacy, if it every had any. Also, it could be

---

[87] *Id.*

argued that because an email is sent to the recipient's email service provider's network until the intended recipient retrieves the message, this is conveying the email to a third party, just like leaving garbage bags out for a trash collector to deliver to a landfill.

C. *Kyllo v. U.S.*[88]

1. Facts

The petitioner was suspected of growing marijuana in his home with heat lamps.[89] From the passenger seat of their vehicle, agents of the United States Department of Interior scanned the petitioner's section of a triplex from across the street with a thermal imager.[90] A thermal imager performs much like a video camera, but it detects infrared radiation that is not visible to the naked eye and converts the radiation into color images based on the amount of heat that is being emitted.[91] The scan revealed part of the petitioner's roof and one of his walls were relatively warmer than the rest of the house and substantially warmer than the other units within the triplex.[92] Based partly on the images from the thermal imager, a warrant authorizing the search of the petitioner's home was issued by a Federal Magistrate Judge.[93] As a result of the search of the home, the petitioner was indicted for manufacturing marijuana.[94] The Supreme Court granted certiorari to determine whether the use of a thermal imager on a home constitutes a Fourth Amendment search.[95]

---

[88] 533 U.S. 27 (2001).
[89] *Id.* at 29.
[90] *Id.* at 29-30.
[91] *Id.*
[92] *Id.* at 30.
[93] *Id.*
[94] *Id.*
[95] *Id.* at 31.

2. Majority Opinion

The Court in *Kyllo* articulated a bright-line rule for this type of surveillance technology, and for technology that will be available in the future.[96] The Court held: (1) when sense-enhancing technology, (2) is used to obtain information concerning the interior of the home, (3) which could only previously have been known by physical intrusion of an area constitutionally protected, and (4) the technology is not in general public use, there is a search for the purposes of the Fourth Amendment.[97] The Court held this search to be presumptively unreasonable unless there is a warrant.[98] The Court reasoned that there is a minimum expectation of privacy in the interior of the home and technology should not shrink that privacy.[99] It did not want the power of technology to shrink the privacy the Fourth Amendment was originally designed to protect.[100]

3. Applying *Kyllo* to Email

In order for *Kyllo* to apply to email, all four elements will need to be met. The technology used to capture email must be sense-enhancing, the information obtained through the surveillance of email must be "regarding the interior of the home," the contents of the email must have been previously discovered only by physical intrusion of an area constitutionally protected, and finally the technology used must not be in "general public use."[101] The sense-enhancing element will likely be met because none of the five senses allow a person to capture information traveling through an Internet connector wire and reconstruct it into a readable document. For the second element, many emails could be considered to be "regarding the interior of the home," but not all. Emails range from the most intimate details of life and home to unsolicited

---

[96] *Id.* at 34-36.
[97] *Id.* at 34.
[98] *Id.* at 40.
[99] *Id.* at 34.
[100] *Id.*
[101] *Id.*

advertisements. A colorable argument can be made that emails of an intimate nature should be considered information concerning the interior of the home. The Court in *Oliver v. United States*[102] said that the area that extends to the "intimate activity of a person's home" is a constitutionally protected area.[103] Even though the Court in *Oliver* was speaking of curtilage, the reasoning could still apply to intimate emails. Many emails will certainly be associated with the intimate activity of a person's home. Whether they are messages of devotion, plans for the children, or announcing dinner time, they all relate to activities that take place within the home and therefore deserve to remain private. But the issue of whether an email that is not "intimate" will fall under the parameters of the *Kyllo* test arises. In striking down the government's argument that the use of a thermal imager is constitutional because it did not disclose intimate details, the *Kyllo* Court said establishing a rule that allows technology to observe any details that are not intimate would be impractical and is not a principle it would follow.[104] Therefore, even if an email is not intimate in nature, it might still be "regarding the interior of the home" and satisfy this element. However, to meet this factor it will likely need to be of some personal nature or at least concern the home in some capacity and not be just an advertisement or mass email in order to fall under *Kyllo*.

Even if an email meets these first two elements, the contents of the email must not be detectable by any means other than physical intrusion without the technology. If an email equates to a first class letter, then the contents of the email will likely only have been discovered by physical intrusion of a constitutionally protected area such as a desk or nightstand in the

---

[102] 466 U.S. 170 (1984).
[103] *Id.* at 180.
[104] *Kyllo*, 533 U.S. at 38.

house.[105] However, as discussed above, the differences between an email and a first class letter might not allow for such a comparison. If not a first class letter, an email will likely be equated to some form of writing, which before could only have been discovered by some physical intrusion. But even if an email was held to be more analogous to a telephone conversation, the Fourth Amendment protection would still be applicable as seen in *Katz*.[106] Finally, the most troubling component in applying *Kyllo*'s holding is the last element: the technology used cannot be in general public use.[107] The Court never defined what is considered "general public use." The dissent in *Kyllo* even pointed out that thousands of thermal imagers were already manufactured and anyone who wanted one could call half a dozen companies to buy one.[108] If the Court did not consider the availability of the thermal imager to be in "general public use," then the fact that any Internet user could obtain a packet sniffer through thousands of websites might not be seen as "general public use" either. But at some point in the future, email surveillance technology, such as packet sniffers, will be so readily available or enough users will have access to other types of technology that the final element will not be satisfied and *Kyllo* will become inapplicable to email, if it is not already. Consequently, as the dissent points out, the threat to the privacy of email will grow as technology becomes more readily available.[109] Surely this is not the effect the Fourth Amendment was designed to have on citizens' rights to be free from unreasonable searches and seizures by the government, nor a precedent the Court would wish to support.

---

[105] *Ex Parte* Jackson, 96 U.S. 727, 733 (1877).
[106] Katz v. United States, 389 U.S. 347, 353 (1967).
[107] *Kyllo*, 533 U.S. at 34.
[108] *Id.* at 47 n.5.
[109] *Id.* at 47.

D. Other Technology Cases

If or when *Kyllo* becomes inapplicable to the interception of email, then other Supreme Court cases that involve technological advancements might be instructive. In *California v. Ciraolo*,[110] the Court held that there was not an objectively reasonable expectation of privacy in a garden of a home from the air and, therefore, the garden could be observed by police officers flying over in a plane.[111] The Court found that the six-foot outer fence and the ten-foot inner fence designed to keep the defendant's marijuana crop from street level visibility satisfied the subjective prong of *Katz*.[112] However, it reasoned that any person flying in public airspace could have observed the plants from above and, accordingly, no expectation of privacy existed even though it was within the curtilage of the home.[113] Similarly, the Court in *Florida v. Riley*[114] held that from a helicopter 400 feet above, police could observe the contents of a greenhouse through open areas in the roof of the greenhouse.[115] Both of these cases illustrate how technology can diminish our Fourth Amendment right to privacy. Before the advent of the airplane and helicopter, a person could expect that their curtilage would be free from the government's eyes if it was sufficiently blocked from view by a fence or greenhouse. Today, because flying is such a common activity, one must also cover the top of his curtilage to be free from snooping eyes, including those of the government.

These are other examples of holdings that when applied to email, will produce alarming results. If hacking emails becomes as common an activity as flying, then the government will likely be allowed to read anyone's email as well. As noted earlier, it is an established principle

---

[110] 476 U.S. 207 (1986).
[111] *Id.* at 214.
[112] *Id.* at 211-12.
[113] *Id.* at 215.
[114] 488 U.S. 445 (1989).
[115] *Id.* at 450-51.

that the government should not be required to avert its eyes from criminal activity that is readily accessible to the general public.[116]

In *Riley*, however, there is a glimmer of hope for protection. In its reasoning, the Court considered that the helicopter did not interfere with the normal use of the greenhouse or any of the curtilage.[117] Accordingly, if the government were to employ a type of email surveillance technology that interfered with the normal use of email, then the use of that technology might be found to be unreasonable. The Court in *Riley* also noted the requirement that no intimate details connected with the home or the curtilage be detected.[118] It might then be possible if an email with intimate details of a person's life is observed during surveillance by the government, the Court will rule this in violation of the Fourth Amendment.

V. Does the ECPA Create a Reasonable Expectation of Privacy?

If one cannot rely on case law to find an expectation of privacy, then it might be possible to look to the statute designed to protect electronic communications in order to trigger Fourth Amendment protection. In light of the changing technology in the field of communications,[119] Congress enacted the Electronic Communications Privacy Act of 1986.[120] This Act extends the reach of Title III of the Omnibus Crime Control and Safe Streets Act to protect against the interception of electronic communications by the government and private actors without prior authorization.[121] It also establishes procedures to gain lawful access to such communications by way of surveillance.[122] Title I of the Act prohibits the interception of electronic

---

[116] California v. Greenwood, 486 U.S. 35, 41 (1988).
[117] *Riley*, 488 U.S. at 452.
[118] *Id.*
[119] United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999).
[120] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).
[121] PATRICIA L. BELLIA ET AL., CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE 238 (2003).
[122] *Id.*

communications, including email, while in transit.[123] Email and other electronic communications that are stored find protection under Title II of the ECPA.[124] Finally, Title III of the Act protects information associated with the addressing and routing of electronic communications.[125]

The relevant inquiry for electronic mail and Fourth Amendment purposes is whether these protections create a reasonable expectation of privacy in email. The district court in *United States. v. Hambrick*,[126] in part held, "[a]lthough Congress is willing to recognize that individuals have some degree of privacy in the stored data and transactional records that their ISP's retain, *the ECPA is hardly a legislative determination that this expectation of privacy is one that rises to the level of 'reasonably objective' for Fourth Amendment purposes*" (emphasis added).[127] Even though the court in *Hambrick* was not ruling on the contents of email, but rather on personal information given to Internet Service Providers by the subscriber, the case is still instructive.[128] The court specifically ruled that Title II of the ECPA did not give a reasonable expectation of privacy in the stored information.[129] This is significant because Title II, as noted above, is the same provision that covers stored email, meaning anything not in transit. Therefore, it is plausible that all stored information does not receive Fourth Amendment protection, including email that has reached its destination. However, the court did hold that some degree of privacy is evidenced by the ECPA, but that this privacy was overridden by the fact that the personal

---

[123] Steve Jackson Games v. U.S. Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994).
[124] *Hambrick*, 55 F. Supp. 2d at 507.
[125] BELLIA ET AL., *supra* note 120, at 257.
[126] 55 F. Supp. 2d 504 (W.D. Va. 1999).
[127] *Id.* at 507 (emphasis added); *see* also United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (holding that the defendant did "not demonstrate an objectively reasonable expectation of privacy in his subscriber information" despite his reliance on the ECPA).
[128] *Hambrick*, 55 F. Supp. 2d at 507.
[129] *Id.*

information was given to a third party: the Internet Service Provider.[130] Accordingly, the ECPA does create a certain amount of privacy for stored email, but it is unclear whether it creates a reasonable expectation of privacy for Fourth Amendment purposes when the email is not given to a third party. However, it could be that every single email is given to a third party because it is actually sent first and stored to the email service provider's server, at least until the message is read by the intended recipient.

Courts have not directly addressed whether the ECPA creates a reasonable expectation of privacy in email that is in transit. If, however, the language of the ECPA is a guide, a reasonable expectation of privacy in email that is in transit might exist because it receives more protection than stored email under the Act. Title II requires a warrant for obtaining a stored email for up to 180 days, but after 180 days it is given less protection.[131] Title I requires a warrant for any email in transit without any time exceptions.[132] Therefore, it is possible that this seemingly small difference in the Act signals a reasonable expectation of privacy for email in transit. In practice, however, this would mean an email is only protected for the few milliseconds it is actually "in transit."

VII. Conclusion

While the courts have yet to clearly decide the issue of whether there is a reasonable expectation of privacy for electronic mail, the Fourth Amendment jurisprudence reasoning is alarming when applied to email. As illustrated by *Greenwood*, *Kyllo*, *Ciraolo*, and *Riley*, as technology increases, privacy will decrease. This will be the trend for email privacy also. If courts follow this reasoning, then the excerpt of Justice Brandeis' dissent in *Olmstead v. United*

---

[130] *Id.* at 508.
[131] Electronic Communications Protection Act of 1986, 18 U.S.C. § 2703(a) (Supp. I 2001).
[132] *Id.* § 2518(3) (2000).

States will become a prophesy that might be fulfilled soon. If there is no Fourth Amendment restraint, then Congress might very well allow the government to capture email without judicial authorization, which essentially will allow the government to reproduce papers in court that were relied upon as secret. Some argue the Patriot Act already allows this.

This is not the spirit of the Fourth Amendment, the intended interpretation of the Amendment by the Court, or the desire of the people. Because the Court has made it clear that the Fourth Amendment protects people and not just areas,[133] this should be the guiding principle in articulating a rule for the privacy of email, rather than the advancement of technology, which continues to shrink privacy. If someday email is regularly intercepted by private actors, the government should continue to respect society's privacy in communication and not be allowed to intercept email as well, at least without first obtaining a warrant supported by probable cause. Law enforcement should not be forced to divert its eyes from criminal activity that is open to the public, but the key words to that well established principle is *criminal activity* – not everyone's email relates to criminal activity. Accordingly, a warrant should always be required before a person's email can be intercepted. An unambiguous rule needs to be set forth to articulate what seems to be the vast majority of email users' belief: that there is a reasonable expectation of privacy in email and, therefore, there is constitutional protection against unreasonable search and seizure.

[133] Katz v. United States, 389 U.S. 347, 353 (1967).