Introduction

Electronic mail (e-mail) is a way of sending text, graphics, and computer files from one computer to another computer. There are three common ways to send and receive e-mail:

1. The sender and recipient might be directly connected as part of a local-area network (now often called an Intranet), which is common on a university campus, company occupying contiguous office space in one building (i.e, a law firm), or industrial park.
2. The sender and recipient might both have accounts at one central computer (e.g., CompuServe, AOL, a privately-owned computer "bulletin board" service, or a computer at a university). The sender and recipient each access this central computer by using a modem and the telephone network.
3. The sender and recipient both have accounts on separate computers that both have access to the Internet. Each party accesses their internet service provider (ISP) by using a modem and the telephone network. Messages between different ISPs are carried on the Internet, which uses high-speed, long-distance telephone network. Examples of ISPs include a private local company or university, or a national service, e.g., UUNet, CompuServe, America OnLine.

Who would want to read someone else's e-mail? Law enforcement agents are interested in communications involving the planning or admission of criminal activity. A businessman is interested in learning proprietary secrets of his competitors. A supervisor is interested in learning about criticism by his/her employees. Agents of foreign governments may conduct espionage on military contractors, diplomatic or defense communications, etc.

There are three situations in which privacy of e-mail could be a concern.

1. Interception during transmission, for example, by a wiretap on the telephone line at the sender's building.
2. Reading during storage on the destination computer. For example, if one sends e-mail to `lstudent@fplc.edu`, this e-mail is stored on a hard drive of a computer at `fplc` until the recipient deletes it. If the recipient does not read the message within a reasonable time, typically a few months of sending the message, the system operator may delete the message to recover space on the hard drive for other users. Good operating practice of a computer system involves making routine backup copies (typically on magnetic tape) of all files on the hard drive, since hard drives can fail. An e-mail may be retrieved from a backup tape *even after* that e-mail was deleted from the hard drive by the recipient.
3. Disclosure of contents by the recipient.

General Statement of the Law

The law regards each of these situations as distinct.

1. Interception of e-mail during transmission is prohibited by federal wiretap statute, 18 U.S.C. § 2510-2521 and also some state wiretap statutes. The federal statutes were amended in 1986 by Title I of the Electronic Communications Privacy Act (ECPA) to include e-mail.
2. Reading e-mail during storage on a computer system is prohibited by federal statute, 18 U.S.C. § 2701-2711, Title II of the Electronic Communications Privacy Act (ECPA), provided that the system is "providing an electronic communication service to the public." This means, among other things, that your e-mail messages are confidential when stored on a computer owned by an ISP that offers to any member of the public the ability to send e-mail and you pay for the account yourself. But there is *no protection* in 18 U.S.C. § 2702 for e-mail stored on a computer system operated by a corporation primarily for its own business communications. So, if you send e-mail to a company (e.g., `jdoe@ibm.com`) and the e-mail is stored on that company's computer, you have no privacy rights under this statute.
3. The recipient of e-mail is generally free to share the information in the e-mail with anyone, subject to legal obligations that are mentioned later in this paper.

Reading e-mail that is stored on a computer is *not* an "interception" under 18 U.S.C. § 2510, et seq., because an interception must be contemporaneous with the transmission of the message between different locations. *Steve Jackson Games v. U.S. Secret Service*, 816 F.Supp. 432, 442 (W.D.Tex. 1993), *aff'd*, 36 F.3d 457, 460 (5thCir. 1994). This holding has been accepted in several subsequent cases, including*Wesley College v. Pitts*, 974 F.Supp. 375, 384-390 (D.Del. 1997); *U.S. v. Moriarty*, 962 F.Supp. 217, 221 (D.Mass. 1997); *Bohach v. City of Reno*, 932 F.Supp. 1232, 1235-36 (D.Nev. 1996).

One court noted that there is a loophole in Title II of the ECPA, where an unknown person can make a copy of e-mail and give it away, then other people who do not provide an electronic communication service can lawfully make a further distribution of copies of that private e-mail. *Wesley College v. Pitts*, 974 F.Supp. 375, 389 (D.Del. 1997).

Extension of old law

Because e-mail is a new medium, invented during the 1970's, there are not many reported cases involving privacy of e-mail. Therefore, attorneys and judges initially looked for analogies in older law. The obvious analogy is voice telephone conversations. Early books on computer law and early law review articles on privacy of e-mail focused on this analogy, to suggest what the law was or should be. However, now, we have several cases interpreting the ECPA, so, when considering privacy of e-mail, cases in analogous areas are mostly of historical importance.

The landmark case of *Katz v. U.S.*, 389 U.S. 347 (1967) considered a wiretap on a public telephone booth. The principal holding in this case was that the police had violated the defendant's privacy upon which he justifiably relied and the police made an unreasonable seizure under the Fourth Amendment to the U.S. Constitution. In Justice Harlan's concurring opinion in *Katz*, 389 U.S. at 361, a two-part test was proposed: (1) Did the person have an actual expectation of privacy in the communication? and (2) Does society recognize this expectation as reasonable? The U.S. Supreme Court accepted this two-part test in *Smith v. Maryland*, 442 U.S. 735, 740 (1979) and restated their acceptance again in *California v. Ciraolo*, 476 U.S. 207, 211 (1986).

Disclosure of contents of e-mail by *the recipient* is not a crime, unless there were disclosure of classified material to *un*authorized persons.

Unless the recipient has some duty of confidentiality (e.g., physician-patient, attorney-client, trade secret disclosed in communication), the recipient is free to share the information with anyone. However, under some circumstances, the sender might sue the recipient for publicity given to private life, under Restatement (Second) Torts § 652D (1977).

If the e-mail were reproduced verbatim, or with only trivial changes, the sender could also sue the recipient for violation of copyright laws. However, if the e-mail was *not* marked with a copyright notice, then the author can only recover the author's actual damages and "any profits of the infringer that are attributable to the infringement", and the defendants can claim "innocent infringement". 17 U.S.C. §§ 401(d), 412, 504(b). Since most e-mail is *not* marked with a copyright notice and the expression in most e-mail is not valuable [There is *no* copyright protection for either ideas or information. 17 U.S.C. § 102(b)], copyright law gives little protection to typical e-mail.

In the special case of e-mail that contains evidence of criminal activity, there is no protection for the confidentiality of the message when the recipient discloses the contents of a communication to law enforcement agents or to a criminal trial. *U.S. v. White*, 401 U.S. 745 (1971)(no violation of Fourth Amendment when defendant spoke to informant who had concealed microphone and transmitter); *Hoffa v. U.S.*, 385 U.S. 293 (1966)(statements made by Hoffa to undercover informant *not* protected by Fourth Amendment). Furthermore, there is no protection under the Fifth Amendment to the U.S. Constitution for production of documents at a criminal trial, *U.S. v. Doe*, 465 U.S. 605 (1984). In summary, the author of an e-mail message generally can not prevent disclosure of the message by the recipient.

Telephone monitoring cases

Two telephone monitoring cases established rules that are relevant to monitoring of employee's e-mail by an employer.

One of the most famous telephone monitoring cases is *Watkins v. Berry & Co.*, 704 F.2d 577 (11thCir. 1983), in which Watkins' supervisor listened to one of Watkins' personal telephone calls. Watkins' employer, the Berry Company, had "an established policy, of which all employees are informed, of monitoring solicitation calls as part of its regular training program." *Id.* at 579. However, this particular call was not an outgoing "solicitation call", but an incoming call from a friend during Watkins' lunch hour. The company's policy, to which Watkins consented, was only to monitoring of sales calls, *not* personal calls. *Id.* at 581. The court stated:

> We hold that a personal call may not be intercepted in the ordinary course of business under the exemption in 18 U.S.C. § 2510(5)(a)(i), except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not. In other words, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents.

Id. at 583.

The court stated that the supervisor

> was justified in listening to that portion of the call which indicated that it was not a business call; beyond that, she was not. Determination of the relevant points [sic] in the call is for the trier of fact. .... We think the conclusion is inescapable that these exemptions [consent and business extension] do not automatically justify interception of an entire call. The expectation of privacy in a conversation is not lost entirely because the privacy of part of it is violated. .... Therefore, [the supervisor] was obliged to cease listening as soon as she had determined that the call was personal, regardless of the contents of the legitimately heard conversation.

Id. at 584. (footnotes omitted)

The holdings in *Watkins* are relevant to a supervisor's viewing of an employee's e-mail, perhaps during inadvertent view of a message on a CRT, or during review of an absent employee's e-mail to ensure the continuity of business operations during the employee's absence.

Three years later, the same circuit court considered a case in which an employee, Smith, overheard another employee in the same room, who was making disparaging remarks on a business telephone about a supervisor. Smith recorded part of the conversation and played the recording to the supervisor. The court held that "this telephone call was not a personal call" – so there was no illegal interception – because

> it occurred during office hours, between co-employees, ... and concerned scurrilous remarks about supervisory employees in their capacities as supervisors. Certainly the potential contamination of a working environment is a matter in which the employer has a legal interest.

Epps v. St. Mary's Hospital, 802 F.2d 412, 417 (11thCir. 1986).

This case makes clear that if an employee wishes to criticize a supervisor, it should not be done using company e-mail. Could criticism of a supervisor be done from home, using a personal

telephone line and a personal e-mail account at an ISP? No, because the recipient of the e-mail could print a copy and show it to someone at the company.

Law of e-mail

Privacy of e-mail was given a statutory basis in 1986 with the passage of the ECPA that provided both criminal and civil penalties for interception of e-mail during transmission (in 18 U.S.C. § 2510-21) and access to e-mail during storage (in 18 U.S.C. § 2701-11).

In addition to the protections in federal statute, an e-mail service (e.g., CompuServe, AOL, bulletin-board operator, or ISP) may explicitly offer written assurance that e-mail messages are private. Such assurances are important for two reasons: (1) they provide a basis for the reasonable expectation of privacy in the *Katz* test and (2) they are an undertaking for breach of which the computer operator may be held liable, either under a warranty claim or tort.

In contrast to privacy of personal e-mail accounts, an employer may monitor e-mail stored on a computer owned by the company, under federal statute. However, it would be prudent for the employer to openly declare to employees this policy of (possibly) monitoring e-mail on the company computer, because such a declaration to employees defeats any claim of privacy under the *Katz* test and weakens the ability of the employees to sue the employer under the common law of privacy.

Note that 18 U.S.C. § 2701 is directed at hackers without authorization, or users who intentionally exceed their authorization, who enter a computer system and then "obtains, alters, or prevents authorized access" to e-mail. Section 2701 is directed more toward computer crime than privacy of e-mail.

Sometimes, attorneys misuse the phrase "e-mail" to describe messages sent to a group of people in a chat room. Such communications to a chat room fail the second part of the *Katz* test, since society does *not* recognize a reasonable expectation of privacy in disclosures made in a public forum. In a chat room, there will be people who are unknown to the author of communications with the chat room, so there can be no legitimate expectation of privacy in a chat room. For example, *U.S. v. Charbonneau*, 979 F.Supp. 1177 (S.D.Ohio 1997) held, in a case concerning a pedophile, that there was no reasonable expectation of privacy in e-mail sent to others in AOL chat room. Use of a chat room must be carefully distinguished from sending e-mail to one person, which *is* a private communication, analogous to a telephone call or first-class letter via the U.S. Post Office.

Privacy of free e-mail

Up to the mid-1990's, there were commonly only two kinds of e-mail: (1) an e-mail service (e.g., CompuServe, AOL) in which each customer pays a monthly fee for access to personal e-mail and (2) e-mail provided by an employer for company business. But in the mid-1990's, a third kind of e-mail became available: free e-mail services provided to individuals by companies like `hotmail` and `Yahoo!`. There is a intriguing question about the privacy of the individual messages in these free e-mail services. On first glance, it would seem that free e-mail services come under the ECPA, 18 U.S.C. § 2701-2711.

But 18 U.S.C. § 2702 specifically limits the protections of criminal law to "a subscriber or customer of such service." But the customer of free e-mail services may be the advertisers who pay for the service,*not* the individuals who use the service. It would be reasonable for a court to interpret "subscriber" to include nonpaying authors and recipients of e-mail.

The interpretation of who is protected by statute is not a specious point. In a different context, it has already arisen in one complicated series of cases. Distributors of illicit drugs tried to move more than twelve million dollars from banks in Texas to banks in New York, using the FedWire e-mail system. The banks in New York had a corresponding relationship with the drug distributors' bank in Columbia. The federal government accessed the e-mail in the FedWire system, seized the money, and instituted forfeiture proceedings. The drug distributors alleged that the U.S. Government violated the ECPA by accessing stored communications. The court noted that 18 U.S.C. § 2707(a) only protected a "provider", "customer", or "subscriber". The e-mail on the FedWire system was between two banks in the USA, and the ultimate beneficiary of the e-mail was *neither* a customer *nor* a subscriber of FedWire. Therefore the court found that the drug distributor had no standing to sue under the ECPA. *Organizacion J.D. Ltda v. U.S.*, 1996 WL 162271 (S.D.N.Y. 1996), *aff'd*, 124 F.3d. 354, 361 (2dCir. 1997). Earlier reported cases in this protracted litigation are reported at 6 F.3d 37 (2dCir. 1993), *cert. denied*, 510 U.S. 1191 (1994) and 18 F.3d 91 (2dCir. 1994).

The statute 18 U.S.C. § 2702 is part of the criminal statute. The right of a civil action arises under 18 U.S.C. § 2707(a), which was amended in 1996 to change "customer" to "any ... other person aggrieved by any violation of this chapter ...." This change clearly gives standing to sue under Title II of the ECPA to authors or recipients of e-mail on free e-mail services.