Global Information Assurance Certification Paper

An Individual's Right to Email Privacy in a Business Environment

GIAC Security Essentials Certification (GSEC)
Version 1.4b

Lee A. Hartmann
March 30, 2003

Many companies have policies regarding email stipulating that the employee's company-provided email account is to be used for business purposes only. However, the user id/password that an employee is required to provide to use his or her email is usually referred to as "private" and "not to be shared with anyone else". This may lead employees to believe that their email is in fact private and encourage them to send email messages that might not be meant for general public viewing. However, this conclusion couldn't be further from the truth.

It is my contention that current laws are unfavorably skewed towards the employer regarding email privacy within the work place. Further, I will argue that such favoritism is an unconstitutional infringement of the employee's Fourth Amendment rights, and illegal under Tort and the Federal Wiretap Law.

Fourth Amendment

The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (U.S. Constitution: Fourth Amendment)." This phrase was initially interpreted to pertain to physical search and seizure only.

Olmstead v. U.S. (277 U.S. 438(1928))

Olmstead v. U.S. was one of the first cases that involved the use of electronic "eavesdropping". During this case, government agents placed taps on the telephone lines leading into Olmstead's offices and the homes of four other suspects. Olmstead argued that under the Fourth Amendment, he had the right to be secure from unreasonable search and seizure and that the federal agents hadn't obtained a warrant for the wiretap.

In a five to four vote, the Court held that wiretaps were not illegal based on the Fourth Amendment. According to the court decision the "well-known historical purpose of the Fourth Amendment, directed against general warrants and writs of assistance, was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects, and to prevent their seizure against his will (Olmstead v. U.S.)." In the opinion of the Supreme Court majority, "search and seizure" referred to physical property and a telephone conversation did not fit within the definition of property. The Court further found that the United States doesn't have any specific policy regarding telegraph and telephone messages as it did in regard to mail going through the postal service.

The court went even one step further, stating that the "common-law rule is that the admissibility of evidence is not affected by the illegality of the means by which it was obtained (Olmstead v. U.S.)." Therefore, even if the Fourth Amendment had been applicable in this matter, the fact that the information had been gathered made it available as trial material.

However, one of the important pieces of this case was the comments made by one of the dissenting judges in this case, Mr. Justice Brandeis. He commented that at the time the Fourth Amendment was written, the Framers could not have foreseen the types of changes new technology would bring and

therefore, could not have phrased the amendment to account for all possibilities. He went on further to point out that a sealed letter is protected by the amendment and the mail delivery is a service furnished by the government. He then noted that telephone service is also a service furnished by the same government and that there is no difference between a sealed letter and a telephone conversation.

Brandeis went even further when he stated, "Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard (Olmstead v. U.S.)." In my judgment, there is little difference between a telephone conversation, a sealed letter, and an email message. If a telephone conversation using an employer's telephone system can be considered private, I would contend that an email message in the same corporate environment should be considered private as well.

However, the court changed its mind regarding the interpretation of the Fourth Amendment in Silverman v. United States.

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

During the Silverman v. United States case, officers pushed an electronic listening device through the wall of an adjoining house until it reached the heating ducts of Silverman's house. This in effect made the heating ducts, which ran through the entire house a listening device.

In this case, the judges found that Silverman's Fourth Amendment rights had been violated. According to Mr. Justice Stewart, "At the very core (of the Fourth Amendment) stands the right of a man to retreat into his own home and be free from unreasonable government intrusion (Silverman v. U.S.)." This was an important decision since it changed the way that the Fourth Amendment had been viewed (as applying only to physical search and seizure), extending its protection to intangible things such as recorded conversations between people without their acknowledgement or consent.

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

During the appeals trial of Katz v. United States, Katz appealed a charge of bookmaking across state lines. FBI agents had bugged a telephone booth that Katz had used to place bets without any written or verbal warrants. The court was found in favor of Katz. Mr. Justice Harlan commented that Silverman v. United States "established that interception of conversations reasonably intended to be private could constitute a 'search and seizure,' and that the examination or taking physical property was not required (for protection under the Fourth Amendment) (Katz v. United States)."

That being the case, why would digital conversation occurring through email be entitled to different legal status than an analog telephone conversation over the same telephone line?

O'Connor v. Ortega (480 U.S. 709 (1987))

In 1987, Ortega appealed the decision of the District Court concerning his lawsuit against O'Connor et al for what he alleged to be unlawful search and seizure. During an administrative leave pending an investigation concerning various allegations against him, hospital officials searched Ortega's office and

seized personal items from his desk and file cabinet which were later used against him in administrative proceedings which led to his dismissal.

Ortega cited his Fourth Amendment rights against the seizure of his private effects. The hospital (O'Connor et al) claimed that Ortega had no right to privacy since his office was on hospital grounds and therefore in a public space not entitled to Fourth Amendment protection.

The judges found that the nature of some offices may make the employee's expectations of privacy unreasonable, but that Ortega had in fact a reasonable expectation of privacy in his office. In the statement made by the judges they stated, "Not everything that passes through the confines of the business address can be considered part of the workplace context (O'Connor v. Ortega)."

Later in the statement they examined the question of "reasonable expectation of privacy", quoting from Katz v. United States, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection (Katz v. United States)." In addition to this, they stated that, "Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis (O'Connor v. Ortega)."

This indicates to me since email accounts are granted to individual users with specific instructions to keep their passwords secret, they may have a "reasonable expectation of privacy" for the messages stored under their ID's. Many companies send confidential information through email without encrypting their messages with the understanding that the information sent through the corporate system is available to the eyes of the intended recipient(s) only. This also encourages the view that individuals have a reasonable expectation of privacy where their work email is concerned.

Electronic Communications Privacy Act of 1986 (ECPA)

In 1986, the Electronic Communications Privacy Act was passed. In section 2511 (1) the Act states that interception and disclosure of wire, oral, or electronic communications is prohibited. Any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication (Sec. 2511. - Interception and disclosure of wire, oral, or electronic communications prohibited)" will be held accountable under law.

While this would seem to offer protection for an email communication, section 2511 (2, a, i) also stated, "It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communications service, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks (Sec. 2511. - Interception and disclosure of wire, oral, or electronic communications prohibited)."

This statement allows an employer to examine email at any time, providing the employer can make the case that examination was necessary to protect company rights or property, or to maintain the system. Given this broad interpretation, almost any search could be condoned, provided that the employer had warned the employee before the fact that company email systems were subject to monitoring incident to normal maintenance or management

This interpretation, in my opinion, unfairly gives the employer the right to go through any piece of email that you send or receive without regard to your constitutional right to a "reasonable expectation to privacy." The judgments in both the Katz v. United States and O'Connor v. Ortega clearly establish that an individual has the right to basic privacy within the workplace that the ECPA clearly disregards.

Bonita P. Bourke et al. v. Nissan Motor Corp. (No. B068705 July 26, 1993 Superior Court of Los Angeles County

In Bourke v. Nissan, two women were hired as Information Systems Specialists to help Infiniti dealerships with their systems and to provide email training. During the training session, one of their co-workers was demonstrating how email worked and randomly sent a message which "was of a personal, sexual nature and not business-related (Bonita P. Bourke et al. v. Nissan Motor Corporation)." The co-worker reported the incident to her supervisor who, with management approval, reviewed all of the email messages from the entire workgroup. During this search they discovered that two women (the plaintiffs) were violating the company policy of using the computer system for personal purposes.

From that point on, the two plaintiffs received poor performance reviews and within a few months, both plaintiffs had lost their jobs with Nissan. During the case, Tort Law was quoted in regards to "intrusion upon seclusion (Bonita P. Bourke et al. v. Nissan Motor Corporation in U.S.A)."

Under this Tort Law principle, intrusion upon seclusion requires proof of an intentional tangible or intangible intrusion into the solitude or private affairs of another that would be highly offensive to a reasonable person. In Bourke v. Nissan, the only email that should have been brought into question was the message that the co-worker forwarded in error. A case could be made that the email was inappropriate and contrary to company policies if any of the people receiving the email message found the message to be offensive. However, the co-worker that received the message didn't complain about the contents of the message until six months after Bourke's termination.

In this case, the court found in favor of Nissan since the EPCA gives employers the right to go through the email of their employees. Although the Fourth Amendment was cited, this argument was considered invalid since the company policy stated that their email could not be considered private and that the company had a right to view it at any time.

Although Nissan had a company policy regarding email use within the company, I would argue that since each user is given a private ID and password to access their account, this gives users a "sense and expectation of privacy". This sense of privacy encourages users to send email to people they trust with

the expectation that the dialogue is of a private nature similar to a phone conversation. As stated in the O'Connor v. Ortega case, everything that passes through a business cannot be considered part of the business itself.

Alana Shoars v. Epson America, Inc. (No. B073234 Court of Appeals of the State of California, Second Appellate District Division Two)

In Shoars v. Epson, Shoars was in charge of providing email training to Epson employees. During this training, she told employees that their email was private and confidential. Later, Shoars discovered that her supervisor, acting on behalf of Epson, was reading and printing employee's email. Shoars protested and her supervisor threatened to fire her if she interfered. Shoars went to her supervisor's boss to protest since she believed that her supervisor's actions were illegal under the wiretapping code (Penal Code sections 630-632.5). Shortly after this incident Shoars was fired.

As with the Bourke v. Nissan case, the court found in favor of Epson. Epson did not have to show any justification as to why they were reviewing their employee's mail. In an article by Cozzetto and Pedeliski , they state "the courts balanced the privacy claims of employees against the legitimate claims of employers. Historically, the courts have permitted incursions into the Fourth Amendment rights of public employees if the intrusions are reasonable, if the employer has a compelling interest, and if the incursions are job-related (Cozzetto, D. and Pedeliski, T.)." I submit that in the case of Epson, the court did not even require Epson to show that they had a compelling reason for the search of their employee's email.

Michael A. Smyth v. The Pillsbury Company

Smyth was fired for sending email to his supervisor that contained derogatory and threatening comments about management. In this particular case, Smyth should have realized that his manager had the right to forward his mail to others that might take offense with the content of his messages. However, Pillsbury had repeatedly stated to its employees that all email communications would remain confidential and privileged. Pillsbury had also publicly stated that email "could not be intercepted and used by the defendant against its employees as grounds for termination or reprimand (Michael A. Smyth v. The Pillsbury Company CA)."

In spite of these reassurances, Smyth was fired for "transmitting what it deemed to be inappropriate and unprofessional comments (Michael A. Smyth v. The Pillsbury Company CA)." Pillsbury never disputed that it had announced that email was confidential, privileged and could not be used as grounds for termination. Smyth still lost this court case. Judge Weiner found that Smyth had no "reasonable expectation of privacy in email communications voluntarily made by an employee to his supervisor over the company email system notwithstanding any assurances that such communication would not be intercepted by management (Michael A. Smyth v. The Pillsbury Company CA)."

This clearly gives the company the right to make any claim to privacy it wants to its employees but provides no burden of justification in breaking that assurance of privacy. Laws provide me with protection in regards to my telephone conversations, my sealed letters, and personal effects that I bring into

the office environment, but no expectation of privacy regarding my email even if email privacy is publicly stated.

Karen Strauss v. Microsoft Corp. (91 Civ. 5928 (SWK))

Companies are citing cases like Strauss v. Microsoft as a valid reason to monitor all employee email. In this case, Strauss sued Microsoft for wrongful termination of employment and sexual discrimination. During the case, email messages from her manager were used as proof of his discriminatory manner. He had sent email to various other people, who in turn forwarded them to Strauss that contained things like "Alice in UNIX Land" and "Mouse Balls".

Additional concerns are sometimes voiced regarding the mode that emails are transferred in. When an email message leaves the company the email address not only has the company's name as part of the return address, the IP (Internet Protocol) number is listed as the mail server's address. This address can easily be traced to the company with tools like 'whois'. Companies are concerned about what employee's might be sending to others with their name and IP address associated with the contents of the message. However, might the same sorts of problems arise with an employee using the company's telephone system or an envelope with the company's return address on it?

Although email messages were used to help prove grounds for sexual discrimination, emails themselves shouldn't be used as an excuse for companies to invade an employee's privacy. The email messages weren't the only proof that the plaintiffs brought to bear in the trail. Various remarks made by the manager were also cited as indicators for sexual discrimination. Email seems more incriminating though since a hard copy can be made and it's not word of mouth.

Title VII of the Civil Rights Act of 1964 is also stated as a reason why some companies are monitoring their employee's email. Companies are tasked by Title VII to create a non-hostile work environment. This includes protecting employees from insulting or threatening messages. According to Cozzetto and Pedeliski, Chevron settled a sexual harassment case out of court for a $2.2 million including as part of the evidence an email that listed 25 reasons why beer was better than women.

They also pointed out that "insensitive comments in a conversation (Cozzetto, D. and Pedeliski, T.)" could also have a detrimental effect. It is possible for employees to plant harassing messages in a phony email trail that the same employee could use later as evidence of sexual harassment or invasion of privacy. Without some way to validate that the message actually came from the person indicated in the message (like a digital signature), email isn't the definitive proof that some would like to claim it to be.

Cozzetto and Pedeliski also point out that in addition to employer worries about Title VII; company's now must also worry about things like copyright infringement. Employees now have the ability to download written materials up to and including entire books, graphics, computer animation, and music. The employer can now be considered as a contributory partner in the infringement suit.

Tort Law

Tort Law may offer some protection of employee privacy. Originating from common law, Tort may offer two different avenues of protection. The first, as mentioned earlier, provides some protection under "intrusion upon seclusion". According to Dekalb, the intrusion must be "substantial and offensive (Dekalb, S.)". Some ways of determining offensiveness may be through context, conduct and circumstance of the intrusion. However, both of these concepts are subjective. What is substantial and offensive to one person may not be for another.

Another area in Tort Law that might offer some protection is under the publication of private facts. Tort gives people the right to not have private facts concerning another person made public when the issue is not legitimate to the concerns of the public and when the act would be highly offensive to a reasonable person. Although there are some things that are generally accepted as "highly offensive to a reasonable person (Dekalb, S.)," such as medical history, family or home life, this phrase gives the judicial system great latitude in judging the degree of the invasion of privacy.

But in order for an employee to use Tort Law in their defense, they must first prove that they are in a private environment. The employee must then also prove that the intrusion was "highly offensive to a reasonable person." But, if the employer can show that they are doing routine maintenance or engaging in a routine practice, then the employee's protest of a private environment becomes invalid. The employer's action would also have to be proven to show some sort of offense towards the employee that would offend the normal person. As stated before, these are highly subjective methods for determining invasion of privacy.

According to Rodriguez, states are free to enact legislation that is more protective than the ECPA but the vast majority of states have chosen to follow the ECPA lead and exempt private businesses providing that they have obtained prior consent of the employee.

Elli Lake, et al., v. Wal-Mart Stores, Inc., et al. (Minnesota Court of Appeals C7-97-263 (July 30. 1998))

Elli Lake and her friend were on a spring break in Mexico. During the trip, she and her friend, Weber, had taken a picture of the two of them standing naked in their hotel shower as a joke. When they returned home, they took their pictures to Wal-Mart to get them processed. When they went to pick up their pictures, they found a notice that the photo of the two of them had not been printed because of its "nature".

Approximately five months later, Lake and her friend Weber were questioned about their sexual orientation from some people that had seen the photo. Upon further investigation, they discovered that a Wal-Mart employee had taken the print of the photo and had shown it to other people. A few months later, the photo was circulating throughout the community. Lake and Weber brought action against Wal-Mart for intrusion upon seclusion, appropriation, publication of private facts, and false light publicity under Tort Law.

Lake and Weber filed a complaint against Wal-Mart in their district court. The district court dismissed the claim with the explanation that Minnesota has not recognized any of the four Tort Laws that the claim was based upon. Minnesota,

North Dakota and Wyoming were the only three states that had not yet recognized any of the four privacy Torts.

Lake and Weber appealed the court decision to the Minnesota Supreme Court. Although Chief Justice Blatz upheld the lower court decision in regards to the intrusion upon seclusion, he reversed the decision based on the other three Torts. He stated that *this court* (Minnesota Supreme Court) had the power to recognize and abolish common law doctrines. Common law "is the embodiment of broad and comprehensive unwritten principles, inspired by natural reason, an innate sense of justice, adopted by common consent for the regulation and government of the affairs of men (Elli Lake, et al., v. Wal-Mart Stores, Inc.)."

This clearly shows that laws need to change and grow with society as it grows and changes. Laws are created to protect the citizens that make up the society. Our society has changed from one based on paper letters that are hand delivered from one point to another, to a society that places much of its correspondence electronically. With this change, we need to make sure that the same protections that were given to paper correspondence are given to their electronic counterparts. Protection of current communication methods needs to stay current with our technology.

Privacy for Consumers and Workers Act (PCWA)

As more and more people enter "cyber space", private citizens are becoming increasingly concerned about their personal privacy. With so much information available to not only the government, but private businesses as well, people want laws passed to protect their electronic privacy.

In an effort to provide more privacy for employees in the workplace, in 1993 the Privacy for Consumers and Workers Act (PCWA) was presented at the Senate and the House. The bill involved a tiered approach to employee monitoring based on length of service to the company. If the employer wanted to monitor an employee's mail during any other time, they would have to show "reasonable suspicion (Rodriguez, A.)" of wrong doing on the part of the employee.

Rodriguez felt that the PCWA failed due to the tiered approach. This approach required the employer to provide advanced notice to the employee that their email was going to be monitored. This made the proposal too inflexible and didn't seem to take into consideration different types of business. For example, some businesses may need to monitor email for legal reasons (stock traders, etc.).

International Privacy Laws

America, land of the free, is lagging behind many European countries in the protection that it affords its citizens. Privacy International states that, "Privacy is a fundamental human right. It underpins human dignity and other values such as freedom of association and freedom of speech (Privacy International)." Most countries around the world acknowledge that their citizens have a right to privacy. An individual's right to privacy is protected in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Our economy has increasingly becoming more global. This means that information being gathered may not be information on people located in the

United States. Countries that have enacted comprehensive laws regarding data privacy, such as the European Union, are concerned about collection of data regarding their citizens by countries that do not have effective privacy laws. Trade may be prohibited or restricted to countries without sufficient data privacy safeguards to ensure the privacy of their citizens (U.S. Department of Commerce).

The European Union (EU) has comprehensive laws regarding data privacy for their citizens. The United States relies on a "mix of legislation, regulation, and self-regulation (U.S. Department of Commerce). The EU does not feel that this mixture of privacy policy provides adequate data privacy protection, and will restrict or prohibit trade with America. A policy called Safe Harbor has been developed to enable American companies to trade with European countries by certifying that their company complies with EU privacy laws. But this does not truly compensate for strong data privacy policies.

According to Privacy International, member states of the EU have "imposed sanctions on numerous countries for failing to regulate wiretapping by government and private individuals (Privacy International)." Safe Harbor provides means for individual companies to continue doing business in Europe, despite differing privacy laws that could otherwise seriously obstruct long-term trade.

Concerns over trying to sue for data privacy infringement half a world away may leave some companies and foreign citizens leery of doing business with us. According to Privacy International, "those countries that refuse to adopt meaningful privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive data (Privacy International)."

International Solutions

In order to create meaningful data privacy, laws need to be enacted on an International basis. An international coalition similar to the United Nations needs to be formed to develop these laws; then an international enforcement agency needs to be created to ensure compliance with privacy laws. Without global privacy protections, our most fundamental human right, privacy, will not be assured. Barriers to free flow of information would also be lowered.

Along with international laws, "data havens", locations where data can be stored without the threat of government oversight, can be established as country independent remailing and URL anonymity sites. This helps to ensure that local governments do not subvert technologies that ensure individual privacy.

Existing Proposals for Improving Employee Email Privacy

Dr. Lee suggests "adoption of a 'flexible' federal policy aimed at preventing unreasonable intrusions relative to varying types of business operations, organizational needs, and employee privacy needs (cited in Rodriguez)." The suggested policy would in many ways reflect the current standard employers have to meet to monitor telephone conversations of their employees. Monitoring must be "reasonable" and have a "legitimate" business need, use the least intrusive methods, limit access to information to only that necessary to meet the objective, and provide reasonable notification of the monitoring and its use.

This is very close to the statement that Justice O'Connor, Chief Justice White, and Justice Powell made in the O'Connor v. Ortega case, "(W)hat is a reasonable search depends on the context within which the search takes place, and requires balancing the employee's legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace (O'Connor v. Ortega)."

Although the name of the commentator is not given, Rodriguez notes another person's argument for language in a policy that would require employers to require a "compelling business interest" before invading the privacy of the employee's email. The unknown commentator further states that by using such wording the "employers will not be able to continue abusive privacy intrusions simply by minimizing employee privacy expectations to the point where courts might consider no privacy interest as having been invaded in the first place (cited in Rodriguez, A.)."

Negotiating Privacy

One of the interesting ideas that Rodriguez brings up is that of negotiating privacy levels with your employer at hiring time. He feels that employee's shouldn't have to give up their right to privacy simply because they are working for a private company. Rodriguez states, "Because the employer-employee relationship is fundamentally contract-based, both parties should be treated as equals at the bargaining table and in the eye of the law (Rodriguez, A.)."

He feels that this negotiated privacy coupled with a federal policy similar to the policy proposed above would benefit both the employer and the employee since expectations of both sides would be explicitly described and would bring privacy from a generic blanket statement down the "individual level". This type of arrangement would help equalize the law that is currently slanted in favor of the employer to the detriment of the employee.

As technology advances towards the point where lines of business and home life blur, companies need to take into consideration the needs of their employees as well as balancing the needs of the company. By involving the employee in the process of negotiating privacy rights, it not only helps to educate the employee, but will most likely gain buy-in into those privacy rights and restrictions as well.

Conclusion

Current laws do not protect an individual's Constitutional right to privacy as granted in the Fourth Amendment, the Federal Wiretap Law, and in Tort Law. The Communications Act of 1986 seemed to strengthen the employer's right to view private email rather than to protect an individual's privacy rights.

As the leading democratic country in the world, we should be doing more to protect our citizens' privacy. Our country should be the world leader in promoting these rights instead of lagging far behind countries that embrace the European Union. If our country won't recognize an individual's right to privacy, businesses who want to do business internationally need to recognize the importance of individual data privacy.

As other countries implement strong data privacy laws for their citizens, they will pressure our country to meet high standards for the protection for their citizens as well as our own. If other countries start to electronically boycott the

United States, changes will be made to protect our piece of the global economy. As long as there are proper safeguards in place, there is no reason to believe that data privacy and law enforcement efforts will be at odds.

Protecting company interests need not be done at the expense of its employees. However this will be difficult to do until laws regarding copy write issues are changed so that the individual responsible for the infringement is held solely accountable for their actions and not the company that they work for. Greed in going after the ones with the "deep pockets" is clouding the party who is truly responsible for the infringement.

In reading the Lawrence Tribe's "prepared" remarks for the First Conference on Computers, Freedom & Privacy held in 1991, a remark he made caught my attention: "New technologies should lead us to look more closely at just **what values** the Constitution seeks to preserve. New technologies should **not** lead us to react reflexively **either way** – either by assuming that technologies the Framers didn't know about make their concerns and values obsolete, or by assuming that those new technologies couldn't possibly provide new ways out of old dilemmas and therefore should be ignored altogether (Tribe, L.)."

This emphasizes to me the difference between the Olmstead v. U.S. and the Silverman v. United States. In the Olmstead trial, judges didn't accord protection under the Fourth Amendment to extend to non-physical things because the exact phrase in the Amendment lists physical items, not eavesdropping. However, in the Silverman case, judges ruled that the original intent of the Fourth did extend to non-physical things like telephone conversations. The judges in that case felt that 'secure in their persons, houses…' meant more than just physical items in a day and age where conversations could be held from a distance and messages were transferred through a telegraph.

There has been much legislation surrounding the protection from wiretaps, telephone conversations, and sealed letters carried by the U.S. Postal Service. These protections are not suddenly dissolved when you go to work at a private company. Email has more similarities to these forms of messaging than differences. So why are employee's privacy rights invaded without any regard to legislation put in place to protect similar methods of communication? I say they are not and should be protected equally under the law.

Bibliography

"Alana Shoars v. Epson America, Inc." No. B073234 In the Court of Appeal of the State of California, Second Appellate District, Division Two. April 14, 1994. URL: http://www.law.seattleu.edu/fachome/chonm/Cases/shoars.html (March 30, 2003).

"Bonita P. Bourke et al. v. Nissan Motor Corporation in U.S.A." No. B068705 In the Court of Appeal of the State of California, Second Appellate District, Division Five. July 26, 1993. URL: http://www.loundy.com/CASES/Bourke_v_Nissan.html (March 30, 2003).

"Communications Act of 1934". June 19, 1934. URL: http://www.usc.edu/~douglast/202/lecture20/1934act.html (March 30, 2003).

"Elli Lake, et al., v. Wal-Mart Stores, Inc.", et al. C7-97-263 State of Minnesota in Supreme Court. July 30, 1998. URL: http://www.lawlibrary.state.mn.us/archive/supct/9807/c797263.htm (March 30, 2003).

"Karen Strauss v. Microsoft Corporation." 91 Civ. 5928 (SWK) United States District Court for the Southern District of New York. (June 1, 1995)

"Katz v. United States" 389 U.S. 347. December 18, 1967. URL: http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=389&invol=347 (March 30, 2003).

"Michael A. Smyth v. The Pillsbury Company CA". No. 95-5712 United States District Court for the Eastern District of Pennsylvania. January 23, 1996. URL: http://www.loundy.com/CASES/Smyth_v_Pillsbury.html (March 30, 2003).

"O'Connor v. Ortega" 480 U.S. 709. March 31, 1987. URL: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=480&invol=709 (March 30, 2003).

"Olmstead v. U.S." 277 U.S. 438. June 4, 1928. URL: http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=277&invol=438 (March 30, 2003).

"Sec. 2511. - Interception and disclosure of wire, oral, or electronic communications prohibited". URL: http://www4.law.cornell.edu/uscode/18/2511.html (March 30, 2003).

"Silverman v. U.S." 365 U.S. 505. March 6, 1961. URL: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=365&invol=505 (March 30, 2003).

"U.S. Constitution: Fourth Amendment". URL: http://supreme.lp.findlaw.com/constitution/amendment04/ (March 30, 2003).

Cozzetto, D. and Pedeliski, T. "Privacy and the Workplace: Technology and Public Employment". (2001) URL: http://www.ipma-hr.org/index.cfm?navid=72&id=793&tcode=nws3&search=1 (March 30, 2003).

Dekalb, S. "The right to privacy in the workplace". (2001) URL: http://www.lommen.com/legal2.asp?RecordNumber=23 (March 30, 2003).

"Title VII of the Civil Rights Act of 1964". (1997) URL: http://www.eeoc.gov/laws/vii.html (March 30, 2003).

Privacy International. “Privacy and human rights 2000 overview”. (2001) URL: http://www.privacyinternational.org/survey/phr2000/overview.html (March 30, 2003).

Rodriguez, A.. “All bark, no byte: employee email privacy rights in the private sector workplace”. (1998) URL: http://eon.law.harvard.edu/privacy/BarkNoByte(Rodriguez).htm (March 30, 2003).

Tribe, L.. “The Constitution in cyberspace”. (1991) URL: http://www.sjgames.com/SS/tribe.html (March 30, 2003).

U.S. Department of Commerce. “Welcome to safe harbor”. URL: http://www.export.gov/safeharbor/ (March 30, 2003).

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event