Emily S. Rose
Professor Tom Armstrong
Computer Science 401
11 March 2015

Employee Email Privacy: Policy and Practice

"If you don't want to see it in the morning paper, don't put it in writing in the first place. The internet is for spreading information, not for keeping secrets." – P. Rose

While most people believe their work email accounts are private and their correspondences will not be viewed by anyone else, this is quite frequently not the case. Messages sent on corporate email accounts are often viewed as property of the employer because the company pays for the accounts. The issue of employee email privacy usually only comes to light upon termination of employment due to employers finding incriminating or inappropriate content in an account's records. Employees who encounter such a situation often press charges for wrongful termination claiming their privacy rights were violated in order to retrieve the information. However, in the absence of laws defining and/or protecting these employees' right to privacy in their email accounts, these cases normally tip in the employer's favor.

Policy:

The United States government has resisted creating specific laws regarding the privacy of electronic communications. Politicians cannot predict what interactions such laws would have with future forms of electronic communications due to the accelerating rate of technological advances. Instead, judges have chosen to assess each email privacy violation claim as a separate and distinct case (Smith & Burg, 2012). Although creating new laws on technology privacy has been largely avoided, the 99th United States Congress enacted the *Electronic Communications Privacy Act of 1986* ("the ECPA") to revise the *Federal Wiretap Act of 1968* to include the protection of "wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers." (United States Department of Justice, 1986) Where the original Wiretap Act only applied to recordings of human voices such as telephone conversations, the ECPA also applies to email and electronically stored data. The ECPA includes two exceptions, both of which require legal authorization. The first exception allows for the authorized[1] interception of "…wire, oral, or electronic communications" and for conducting electronic surveillance. The second allows a government worker or department to apply for a court order authorizing the installation and use of either a pen register[2] or a tap and

[1] "Operators and service providers for uses "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service" and for "persons authorized by law" " (United States Department of Justice, 1986)

[2] "A device that captures the dialed numbers and related information to which outgoing calls or communications are made" (United States Department of Justice, 1986)

trace[3] by certifying that the information that will be gathered is "relevant to an ongoing criminal investigation being conducted by the applicant's agency" (United States Department of Justice, 1986).

The ECPA has been amended by the United States government multiple times since its enactment, the most notable amendment being the USA PATRIOT Act of 2001 (United States Department of Justice, 1986).

Practice:

Why would an employer be interested in reading their employee's mail? There are many different answers to this question. A supervisor may be concerned with the amount of paid time one of their employees is using for personal business, a company's human resources department may be investigating a report of harassment against an employee, or an automated system may have flagged an email sent by an employee, causing the company to investigate further by examining other emails sent and received by the account.

There are countless reasons why a business may look into their workers' correspondences, so what rights do employees have? How does the court determine whether or not the plaintiff's right to privacy was violated? The first major court case to dispute this question was *Katz v. United States* in 1967, where the evidence brought against Katz was obtained by the FBI by using a wiretap on the public phone booth Katz was using without first obtaining a warrant (Katz v. United States, 1967). From this case, a two-step test was created to determine if Katz's privacy rights were violated. The first step required Katz to prove he had an actual expectation of privacy and the second was determining whether the defendant (FBI) had sufficient reason perform the search (Smith & Burg, 2012). Katz proved he had a reasonable expectation of privacy because the telephone booth was public and there were no postings informing users that it was under surveillance. For the second step, it was determined that placing a wiretap on a public phone booth without a warrant is a violation of the 4th amendment because it is an unreasonable search of private property.

This two step test has been used in many technology privacy cases but becomes much more complicated. For example, businesses may attempt to take away their employees' expectations of privacy by including monitoring policies in their employee handbooks or by disallowing personal use of company technology, but if the employer does not follow through with these policies regularly or leads their employees to believe the policy enforcement differs from what is written, the employee may maintain a reasonable expectation of privacy. On the other hand, any information stored in/on company property, such as an email server or a computer, may be considered property of the employer. These are just a few examples of the many reasons that specific laws have not been created to handle electronic communications (Smith & Burg, 2012).

---

[3] "A device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated." (United States Department of Justice, 1986)

The employer usually comes out on top in cases of employee email privacy because corporate email accounts are property of the company. This is not to say, however, that employers regularly monitor the corporate email accounts. For example, the University of Rhode Island regularly monitors both employee and student email accounts, but the University uses an automated system to detect outgoing spam and sensitive data instead of allowing other employees to monitor the accounts. University email accounts are only accessed by humans in "cases involving a court order" or "a request by the head of Human Resources," the latter of which allows mail administrators to "go into a user's email account to look for evidence of criminal activity or violation of policy" (Rose, 2015).

By discussing company privacy and technology policies with your supervisor, you can develop an understanding of how much privacy you may have. These discussions will result with one of the two following possibilities: you may leave the conversation with what can be considered to be a reasonable expectation of privacy, which would most likely hold up in a court of law if anything were to happen. You may instead end the conversation with an understanding of the policies and practices the company has, enabling you to avoid putting yourself in a problematic situation in the first place. In the end, more information is better. By gathering information about your company's policies and practice around employee privacy, you can better protect yourself for the future.

Bibliography

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

Rose, P. G. (2015, March 4). Email Monitoring at the University of Rhode Island. (E. Rose, Interviewer)

Smith, D. V., & Burg, J. (2012, November/December). What Are the Limits of Employee Privacy? *GPSOLO, 29*(6).

United States Department of Justice. (1986, October 21). *Electronic Communications Privacy Act of 1986.* Retrieved March 5, 2015, from Justice Information Sharing: https://it.ojp.gov/default.aspx?area=privacy&page=1285