

Monitoring Employee Communications In Cyberspace: The Pitfalls Facing Management

August Bequai

Legal Editor

7921 Jones Branch Drive, Suite 133, McLean, Virginia 22102, USA

Introduction

Cyberspace has changed the way modern organizations communicate and conduct their daily business. Cyberspace is also fast changing the employer-employee relationship. A survey of 1000 US corporations found that management, in nearly two-thirds of them, routinely reviewed employee E-mail, taped telephone conversations, tracked the number of keystrokes on computers, and took other measures to monitor the work-habits of their employees. A growing number of businesses now use the Internet to track the movements and location of their employees.

Few will dispute that cyberspace has given rise to new markets and business opportunities. Likewise, few will dispute that cyberspace has also given rise to a plethora of legal concerns; as well as exposing management to an array of legal liabilities in the current litigious environment. For example, when two employees of a Wall Street brokerage firm were found to be using their company's E-mail to transmit offensive and vulgar images, some of their co-workers sued management. Litigation as it relates to Cyberspace, is on the increase.

Taping Communications

Many US corporations monitor E-mail and related communications for purposes of quality control and to document legitimate business transactions. But the monitoring of employee communications frequently involves the interception of "wire communications," as these terms are defined by the US wiretap laws. Under both federal and state wiretap laws, at least one of the parties must consent for the interception to be lawful. Employees who run afoul of these laws, do so at their own peril.

The federal wiretap laws do not prohibit the taping or monitoring of telecommunications by a person who is a party to, or has the prior consent of, at least one of the parties to the conversations, unless the taping is carried out for the purpose of committing (or attempting to commit) a criminal act. However, the prohibition against criminal acts does not apply if the consenting party's purpose was to preserve an accurate record of the communication. But the prohibition will apply where, for example, the determining factor in the consenting party's purpose was to engage in blackmail, extort money or force the settlement of civil litigation.

Monitoring Employee Communications In Cyberspace: The Pitfalls Facing Management/August Bequai

The legislative history of the US “Omnibus Crime Control and Safe Streets Act” makes it clear that an employer who is not a party to the employee communication, has no authority to provide the necessary consent; even though the employer is a subscriber of the communication service. Neither can an employer compel its employees to consent. While advance notice to employees is required by many of the state wiretap laws, there is no requirement that they expressly consent to the monitoring.

The judicial test for an implied consent is less rigorous than for the consent to the waiver of an employee’s Constitutional rights. It merely requires that the communication can be the subject of monitoring. A consent is not viewed as involuntary merely because it is induced by promises of leniency or immunity; nor does a consent become involuntary because it is requested by a law enforcement agency. However, the mere fact that the monitoring results from an employer’s policies and serves its interests, will not suffice to prove duress.

At the local level, many of the states have adopted different standards from the US Government with regard to consensual wiretaps. Some states require the consent of all parties to the communication; while others require consent by only one of the parties. This local legal patchwork exists because the US Congress, when it passed the federal wiretap laws, allowed for concurrent state regulations.

The federal wiretap laws also make it illegal to intercept telecommunications; as well as allowing recovery for actual damages and other losses resulting from these violations. The wiretap laws also provide for punitive damages and attorney’s fees. Some of the state laws follow the federal lead, and provide for attorney’s fees. However, many of the state wiretap laws do not recognize an action for invasion of privacy.

For management to circumvent the trappings of the wiretap laws, it should design policies that meet its business purposes; which are in conformity with both federal and state laws. Their objective should be to appear as if management acted reasonably in balancing its legitimate business needs against the privacy

rights of its workforce. Management should be in a position to demonstrate to a court, that a legitimate business need were the motivation for the interception.

But prior to the implementation of any such policies, written notice should be provided to the workforce; summarizing management’s policies as to employee communications. Notice should also be given to all new hires, consultants, and other third parties that provide services to the organization. Copies of the notice should be included in the personnel files of these individuals, so as to document compliance by management with the law. Management should also insert such notices in the employee manual and other policies and procedures that are periodically circulated to the staff.

The purpose of the notice is to legally establish the implied consent of all parties that participate in the recorded or monitored communications; satisfying the minimum legal requirement of one-party consent. At the same time, the employee’s expectations of privacy are curtailed. Management should also update its policies regarding personal or private communications after business hours, if such communications are carried out on corporate facilities or equipment.

While two-party consent is not required in the majority of jurisdictions for the interception of employee communications; management enjoys additional legal safeguards if the employee knowingly participates, after being placed on notice. The employee cannot claim a reasonable expectation of communication privacy once it is placed on notice. The defence of consent will prove effective in the event of an invasion of privacy lawsuit by the employee.

Privacy In Cyberspace

Prior to 1986, the federal wiretap laws did not cover any computer-related communications. The US Electronic Communications Privacy Act of 1986 changed all this, and amended the federal wiretap laws to cover the interception of computer-related exchanges. The Act’s prohibition against interceptions provides for the privacy of computer-related transmissions.

The Act also covers access to and the disclosure of data in storage. Under the Act, there can be no interception of computer communications once the data is in "electronic storage". The definition of "electronic communication" under the Act, does not encompass the storage of data. Under the Act, the term "electronic storage" includes only the temporary or intermediate storage of a communication; incidental to its transmission and storage by an electronic communications service as backup data. Accesses to computer communications that have a transmission and storage phase, are governed by different provisions of the federal wiretap laws. This legal void has led some courts to observe that the same message is subject to differing standards of protection merely because it exists in a different statutorily defined medium.

However, the judicial interpretation of the existing federal wiretap laws continues to evolve. Most provisions of the Act remain untested in the courts. Currently, most jurists view the Act as allowing employers to monitor the E-mail of their employees. While legislation has been periodically introduced in the US Congress to limit such monitoring, to date, it has not passed.

Under current US law, a corporate provider of private communication networks is allowed to intercept employee messages as long as there is a business purpose for it to do so. The so-called consent exception, traditionally applicable to telephone communications, has been extended to computer communications; specifically, that there be prior consent or approval by at least one of the participants to the communication.

The same monitoring practices that have traditionally been applied to telephonic communications in the US, are now being extended by the courts to in-progress computer exchanges. Employer liability is unlikely if it can be shown that there is a legitimate business purpose for the monitoring; further, that notice of the monitoring was given to the workforce. The actions are consistent with existing monitoring policy, and personal communications can be monitored only to the extent that is necessary to determine their nature and not their contents.

Gaining access to stored data is not viewed as an interception by most US courts; nor is the replaying of previously recorded communication. Likewise, the accessing of stored private E-mail, not yet retrieved by its recipients, is not considered an intercept.

The Act also makes it unlawful to access stored electronic communications without authorization or in excess of authorization. The conduct is not unlawful if the access is pursuant to authorization by the person or entity providing a wire or electronic communications service. Since an employer can be viewed as such a provider, it will be allowed to write its own standards regarding access to its stored data.

The federal "Computer Fraud and Abuse Act" and related state computer laws, criminalize conduct that involves unauthorized access or access in excess of authority, to a computer or computer network. Under these laws, the use of a computer to invade a third party's privacy is made a crime. Thus, a person would be guilty of a crime if he or she uses a computer to examine, without authority or in excess of authority, any employment, salary, credit or any other financial or personal information relating to any other person. The conduct is immunized if the access is pursuant to permission from the owner or lessee of the computer network or program.

Unauthorized access or disclosure of stored communications can result in civil liability under the wiretap laws. The culprit can be ordered by a court to pay the sum of actual damages and any profits realized from the violation; as well as reasonable attorney's fees and court costs. The unauthorized access to data stored in a computer or computer network can also give rise to civil liability for invasion of privacy under state computer crime laws. The latter authorize a private action for any damages sustained or any losses of profits.

Under current law, access to employee medical information is restricted to personnel with a lawful need to know. Federal law requires that medical data be maintained in secure and segregated files. Restricted access should serve to ensure its privacy, by preventing the review of sensitive medical data by co-workers and other third parties. Responsibility for accessing such

Monitoring Employee Communications In Cyberspace: The Pitfalls Facing Management/August Bequai

data, should rest with an administrator who can identify legitimate business applications.

Access to data should be governed by the rule of law. It should be restrictive enough to safeguard privacy; while sufficiently flexible to allow its legitimate business use. For example, both the personnel and payroll department frequently require access to salary data. There is also a legitimate business need for retaining credit and financial data. Businesses also have an operating need to retain current garnishment information on their employees. However, they do not have a legal right to retain data long after compliance or cessation of employment by the individual in question.

Privacy concerns may also exist as the result of collective bargaining agreements between employees and their labour organizations. These agreements will frequently restrict access by the employer to its employee files or communications. As a practical matter, a company's data access policies should reflect its own interests in restricting access to proprietary data; as well as any contractual undertakings it has to third parties. The monitoring of Internet communications by an employer, thus, would need to conform to these restrictions in order to pass the legal litmus test.

Internet Security Policies

In the age of the Internet, management needs to establish data security policies and procedures that

address its needs; with minimal privacy intrusions. By so doing, management can, thus, raise the defence that it acted reasonably and in conformity with legitimate business needs.

The workforce should also be placed on advance notice that the Internet and related online systems are to be used solely for business purposes, whenever company time and equipment are involved. In-house mechanisms should be established to address questions and grievances related to these employees.

Periodic reviews of E-mail and online systems should also be carried out to confirm that they are being used by the workforce in accordance with company policies and procedures. Internet security policies should also be reviewed to ensure compliance with federal and state legal requirements.

Summary

While cyber-monitoring of employee Internet communications by employers is lawful when carried out in conformity with existing wiretap and privacy laws, nevertheless, management needs to exercise restraint; as well as enact data policies and procedures that are in conformity with federal and state privacy laws. Ultimately, how management conforms to these privacy laws, will impact on the evolution of the cyber-revolution.

August Bequai, Esq. is a McLean, Virginia attorney and the author of numerous books and articles.