Denver Law Review

Volume 79
Issue 4 *Symposium - Privacy*

Article 2

January 2002

Job Insecurity - When It Comes to Workplace Surveillance of Electronic Communications, Employers Are Free to Establish the Rules of the Game

Philip L. Gordon

Job Insecurity - When It Comes to Workplace Surveillance of Electronic Communications, Employers Are Free to Establish the Rules of the Game

JOB INSECURITY?

When It Comes To Workplace Surveillance Of Electronic Communications, Employers Are Free To Establish The Rules Of The Game

by Philip L. Gordon, Esq.

Introduction

In May, 2001, when federal judges on the United States Court of Appeals for the Ninth Circuit learned that, in at least one important respect, they were no different from millions of clock-punchers worldwide, they were outraged.[1] What was the startling revelation for these usually imperturbable appellate court judges? Mere bureaucrats in the Administrative Office of the United States Courts, a little known group of civil servants who administer the federal court system, were monitoring the federal judiciary's e-mail and Internet traffic, including the traffic of these Article III judges.[2] The perceived intrusion upon the seclusion of judicial chambers so incensed Judge Alex Kozinski that he took the highly unusual step of publicly denouncing the chief of the administrative agency in the *Wall Street Journal* and discussed his views on a nationally televised talk show.[3]

Ironically, in the years preceding this millennial epiphany, judges, practically all of whom came of age with the rotary dial telephone, had put in place a regime which has made it extremely difficult for workers to recover damages based upon their employers' review of e-mail and Internet communications. This situation has resulted from a judicial construction of the Federal Wiretap Act,[4] which effectively eliminates any statutory privacy protection for workplace e-mail and Internet use. With e-mail and Internet use steadily transforming the United States Postal Service into a quaint relic, the time is ripe for judges, and Congress as well, to re-think the law governing the privacy of e-mail and Internet communications. However, the events of September 11, 2001, have placed the issue of workplace privacy on the judicial and legislative backburner.

Consequently, employers, who are increasingly concerned about regulating the use of e-mail and Internet in the workplace, should view this regulatory vacuum as an opportunity to establish their own rules governing the use of these resources.[5] Moreover, employers have a range of electronic monitoring policies from which to choose. At one end of the spectrum is a policy aimed at protecting employers from abuse of their electronic communications systems through employee consent to unrestricted electronic monitoring. At the other extreme is a policy based upon the principle that electronic privacy should be a workplace benefit. Employers can tailor either policy to meet their own specific needs and the demands of their particular workforce.[6]

From The Rotary-Dial Telephone To The Apple Macintosh: The Evolution Of The Federal Wiretap Act

The 1960s were watershed years for wiretaps. By that time, tapping technology had been in use for decades with practically no restrictions or judicial oversight under federal law.[7] Then, the United States Supreme Court revolutionized the notion of communications privacy. In *Katz v. United States*,[8] the Court held that even someone who uses a public telephone booth can have an objectively reasonable, subjective expectation of privacy in the content of his telephone call, an interest protected by the Fourth Amendment from government intrusion.[9]

Congress responded to *Katz* by outlawing virtually all interceptions of telephone calls without judicial

authorization. Congress also strictly limited the circumstances in which a court could order a telephone wiretap.[10] However, the statute embodying this regime, the Federal Wiretap Act, was a creature of its time. The statute was premised upon a monolithic communications world inhabited only by AT&T and its copper telephone lines.

In the opening years of the 1980s, the world upon which the Federal Wiretap Act was premised changed slowly, but radically. Apple Computers began to market "The Macintosh," the first computer designed for consumption by the general public. Electronic mail was becoming a widespread means of communication. The cordless telephone represented the cutting edge of telephone technology. The answering machine had just recently become a "must-have" commodity. The divestiture of AT&T was a work in progress.

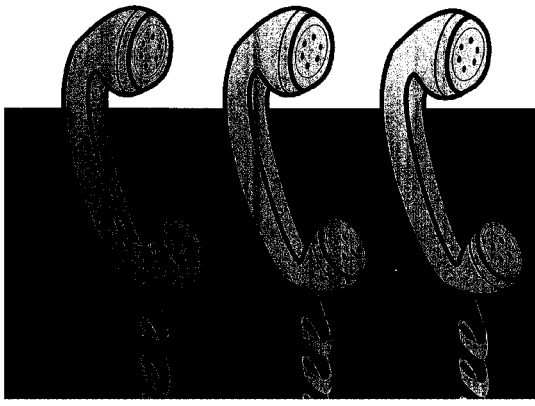
With this backdrop, Congress amended the Federal Wiretap Act in 1986, thereby extending the Act's coverage to "electronic communications."[11] In contrast to "wire communications" - transmissions of the human voice over telephone lines - "electronic communications" encompassed transfers of data not containing the human voice[12] (Napster, of course, was not yet on the radar).

At the same time, Congress passed an accompaniment to the Federal Wiretap Act, which sometimes is referred to as the Stored Communications Act.[13] This statute protects stored electronic communications in two limited respects. First, an anti-hacking provision prohibits unauthorized access to "a facility through which an electronic communication service is provided," such as a server, for purposes of obtaining access to electronic communications stored in that facility.[14] Second, the statute imposes upon those who provide electronic communications services to the public, such as an Internet Service Provider ("ISP"), an obligation to maintain the privacy of electronic communications stored on their own servers.[15]

The Judicial De-Clawing Of Federal Statutory Protections For The Privacy Of E-Mail And Internet Communications

The practical effects of this dichotomy between electronic communications and stored electronic communications became apparent only as claims under the Federal Wiretap Act based upon the unauthorized review of e-mail began to trickle through the judicial pipeline. The seminal case in the area, *Steve Jackson Games, Inc. v. United States Secret Serv.*,[16] did not involve workplace monitoring, but rather the Secret Service's review of un-retrieved e-mail stored on the hard drive of a computer seized from a company offering an electronic bulletin board service.[17] The United States Court of Appeals for the Fifth Circuit held that the Secret Service's conduct was not actionable under the Federal Wiretap Act because the Act prohibits only "real-time" interceptions of electronic communications, i.e., the acquisition of the content of the communication *while the communication is in transmission.*[18] Because the e-mail reviewed by the Secret Service was in electronic storage, the Federal Wiretap Act did not apply. However, the Secret Service did not escape *Steve Jackson Games* scot-free. The Fifth Circuit's opinion notes that the Secret Service did not challenge the district court's finding that its agents had violated the Stored Communications Act by reviewing the un-retrieved e-mail without authorization from the service provider, without the consent of either party to the communications reviewed, and without judicial authorization.[19]

Steve Jackson Games opened the door to unrestrained monitoring of workplace e-mail and Internet use. Until relatively recently, software capable of "real-time" interception of e-mail and Internet communications was not even commercially available. Consequently, employers seeking to monitor employee e-mail and Internet use had no choice but to retrieve the content of those communications from electronic storage on the



" The statute was premised upon a monolithic communications world inhabited only by AT&T and its copper telephone lines."

employer's server. Moreover, unlike the Secret Service in *Steve Jackson Games*, an employer can not be held liable under the Stored Communications Act for retrieving employee e-mail from its own server because that statute expressly excludes the system provider from liability.[20] The Stored Communications Act also is inapplicable to an employer's retrieval of e-mail permanently stored on an employee's hard drive because the Stored Communications Act protects electronic communications only when in intermediate or temporary storage.[21]

The Fifth Circuit's construction of the Federal Wiretap Act to prohibit only "real-time" interception of e-mail and Internet use dominated the judicial scene until the United States Court of Appeals for the Ninth Circuit addressed the issue in January 2001.[22] Perhaps as a precursor to its outcry against e-mail and Internet monitoring by the Administrative Office of the United States Courts, the Ninth Circuit in *Konop v. Hawaiian Airlines*[23] held that the acquisition of the content of an electronic communication may be actionable under the Federal Wiretap Act even if the electronic communication is not in transmission when the acquisition occurs.[24] In that case, Konop, an airline pilot, maintained a closed bulletin board for pilots to speak critically about both union representatives and company officials.[25] Konop alleged that an airline executive violated the Federal Wiretap Act by using false pretenses to obtain access to, and to review, messages on the bulletin board.[26] The Ninth Circuit, rejecting the Fifth Circuit's construction of the Act in *Steve Jackson Games*, held that the airline executive's actions constituted an interception under the Act.[27] Relying in part upon its holding in *United States v. Smith*,[28] that the unauthorized retrieval of a voice mail message constituted an interception under the Federal Wiretap Act,[29] the *Konop* court stated that there was no reasoned basis for distinguishing between voice mail and electronic mail.[30]

Philip L. Gordon is a shareholder in the Denver office of Littler Mendelson, P.C., a national labor and employment law firm, and a fellow of the Privacy Foundation. Mr. Gordon specializes in counseling employers on privacy issues and representing employers in privacy-related litigation

The proponents of workplace privacy had a short-lived victory. In a startling reversal, revealed shortly before the September 11 terrorist attacks, the panel in *Konop* withdrew its opinion *sua sponte*, with one judge dissenting.[31] The majority's brief opinion provides no reason for this highly unusual action.[32] The majority might have belatedly realized the potential impact of the panel's original decision on law enforcement, thus explaining the panel's hasty retreat from its novel holding. If the retrieval of stored e-mail does constitute an interception under the Federal Wiretap Act, then law enforcement authorities must obtain court authorization and comply with the Federal Wiretap Act's stringent limitations on interceptions before, for example, obtaining access to e-mail on an ISP's servers. By contrast, the Stored Communications Act, which otherwise regulates access by law enforcement officials to electronic communications in storage at an ISP, establishes a much lower threshold and much less stringent requirements for access to stored electronic communications.[33]

Congressional Reconstruction Of Federal Privacy Protections For E-Mail And Internet Use Is Not On The Horizon

The prevailing statutory construction leads to bizarre results in the employment context. Communications by telephone — whether wire-line, cordless, or cellular — enjoy full protection under the Federal Wiretap Act.[34] Federal law also protects the most obvious piece of junk, snail mail, from unauthorized interception.[35] By contrast, under *Steve Jackson Games* and its progeny, electronic mail enjoys no protection under the Act unless intercepted in real-time.[36] Put another way, employers cannot obtain the contents of telephone communications in any form without risking liability under the Act, but employers can review employee e-mail and Internet use with impunity so long as they do not intercept the content of the communication in real-time.[37]

This is not the first time that the Federal Wiretap Act has resulted in an arguably irrational stratification of means of communication. In 1986, when Congress expanded the Federal Wiretap Act to encompass "electronic communications," Congress contemporaneously and expressly excluded cordless telephone communications from the Act's coverage.[38] Congress reasoned that the general public could readily attain the radio portion of a cordless telephone conversation that resulted from the transmission between the handset and the base unit. Consequently, the cordless telephone user could not have an

objectively reasonable expectation of privacy in his cordless telephone conversations.[39]

This "cordless" exclusion, like the real-time construction of the word "interception," resulted in a boon for law enforcement. Numerous reported cases decided under the Federal Wiretap Act after 1986 analyzed motions filed by criminal defendants to suppress the contents of cordless telephone conversations acquired by a police scanner, or even a neighbor's baby monitor.[40] Relying on the Congressional exclusion, courts uniformly denied these motions to suppress, whether based upon the Act or upon the Fourth Amendment.[41]

Notwithstanding this law enforcement benefit, Congress eliminated the "cordless exclusion" in 1994.[42] Congress concluded that the distinction between unprotected calls over cordless telephones and protected calls over cellular and wire-line telephones had become untenable. Even though it was commonly known that others could easily acquire the radio portion of a cordless telephone call, the use had become so widespread that society could no longer tolerate unrestrained interceptions of this means of communication.[43]

A similar congressional reversal of the distinction between wire communications and electronic communications resulting from the judicial construction of the term "interception" is not on the horizon. In the wake of September 11th, Congress probably will not amend the Federal Wiretap Act to put the interception of stored electronic mail on an equal footing with the interception of telephone calls. To do so would impose new constraints on law enforcement when society is focused on the war on terrorism and the need to ensure personal security.

If anything, Congress signaled its approval of the judicial distinction between real-time interception and retrieval from storage when it passed anti-terrorism legislation in October 2001, popularly known as the USA Patriot Act. That statute, among other things, removed voice mail from the scope of the Federal Wiretap Act.[44] As a result, telephone calls, like electronic mail, now enjoy federal statutory protection only when intercepted in real-time.

How Employers Can Fill The Judicial And Legislative Vacuum

Until Congress takes action, the e-mailer's situation today will remain similar to the man in the sidewalk telephone booth in *Katz*, or the cordless telephone user between 1986 and 1994. The means of communication has become a part of everyday life but its use is potentially perilous.

From the employer's perspective, this situation has advantages in the workplace. The e-mail system can pose a potential threat by, for example, allowing the transmission of trade secrets off site with the press of a button. In addition, Internet use can interfere with the intended business purposes of the employer's system resources through, for example, the downloading of pornography. Also, the circulation by e-mail of provocative messages could raise the specter of discrimination or sexual harassment claims. Given these risks, employers are appropriately concerned about these abuses and their potential costs. In the absence of judicial or legislative limits, employers have the freedom to protect themselves from these risks as long as they do not intercept the content of electronic communications in real time without first obtaining their employees' consent.[45]

By the same token, unrestricted electronic monitoring may stifle beneficial uses of e-mail and the Internet. Privacy spawns creativity, and the rapid interchange of ideas through e-mail can accelerate the creative process. But, if an employee fears that a supervisor who monitors the mail will swat down an unorthodox idea, she might be less willing to express herself. With respect to personal activities, a modicum of privacy may ultimately benefit the employer. After all, which course of conduct is more efficient: fifteen minutes of surfing Amazon.com's Web site or one hour on a secret mission to Barnes & Noble located several blocks from the office?

This question remains: how should an employer regulate the use of e-mail and the Internet in the workplace? The answer will depend upon an array of factors including, for example, the employer's own objectives, the maturity and sophistication of the employer's workforce, the function of e-mail and Internet communications in the particular workplace, and whether trade secrets are accessible in electronic format.

Those employers who view their electronic communications system as a threat could deter abusive conduct with a policy designed to send a clear signal to employees that if they abuse the employer's system, they will be caught and disciplined. Some of the principal points of this type of policy would state the following:

1. The electronic communications system and all communications sent, received, or stored by the system are the property of the employer;

2. The employer reserves the right to monitor, read, copy, print, and distribute the content of all electronic communications, including e-mail and Web sites visits, sent, received, or stored by the system;

3. How the monitoring will be effectuated;

4. By signing the employer's

continued on page 575

continued from page 516
monitoring policy, the employee consents to the employer's monitoring of the content of all electronic communications sent, received, or stored by the system;

5. When using the electronic communications system, employees should always keep in mind that others may view their communications, therefore employees should use discretion when sending e-mail and making Web visits;

6. Employees are not authorized to use any computer password unless the password is revealed to the employer;

7. Personal use of the employer's electronic communications system is not permitted;

8. The following are impermissible uses of the system: transmission of sexually oriented or ethnically derogatory materials, unauthorized distribution of trade secrets or confidential information, and unauthorized copying of copyrighted material;

9. Any violation of the policy may subject the employee to discipline, up through and including termination;

A different electronic monitoring policy should be put in place by employers with less concern about potential abuse and a philosophy that their corporate mission will benefit from a workforce who can communicate freely by e-mail or over the Internet. This type of policy would guarantee the privacy of certain communications while preserving the employer's ability to police the system and to punish abusers. A policy embodying this approach might include the following elements:

1. The types of personal uses that are permissible and impermissible;

2. The amount of personal time allowed;

3. The time of day that personal use is permitted;

4. That permissible, personal e-mail and Internet use will not be monitored absent justification for doing so;

5. The security measures that will be taken to protect the privacy of personal e-mail and Internet use;

6. An explanation of the type of monitoring technology used to prevent impermissible personal use;

7. How frequently employees will be monitored;

8. The consequences of violating the policy.

There is one caveat for an employer who opts for this "privacy-as-a-benefit" approach. A failure to honor the policy might open the employer to liability for tortiously intruding upon the private space created by the employer or for breach of an implied contract.

Regardless of the type of policy the employer decides to adopt, a document retention/destruction policy should accompany any electronic monitoring policy. The former policy should be designed to assist the employer in managing the enormous quantity of information stored in its computer systems. At the same time, this policy should reduce the cost of responding to "electronic discovery" and reduce the risk that a "smoking-gun" e-mail will remain stored on the employer's system. The policy should address the following:

1. Classifications of data compatible with search capabilities;

2. Segregation of privileged communications and trade secrets;

3. The period for data retention, bearing in mind the type of data in question and any applicable legal requirements;

4. Strict limits on the retention of personal e-mail;

5. Application of the policy to all corporate computers (e.g., local, network, and back-up storage) and to computers of employees leaving the company.

Document destruction, no matter how well intentioned, almost inevitably will spur allegations of bad faith when litigation does arise. To deter such allegations, the policy should be developed and implemented long before litigation is on the horizon. In addition, the employer should maintain all documents bearing upon the creation and implementation of the policy. Finally, the policy should be consistently enforced, and suspended and reviewed when litigation is imminent.

Conclusion

The American workforce continues to use a growing array of communications tools to the benefit of employers. Some of these tools, like e-mail and the Internet, contemporaneously create unprecedented risks for employers. The existing statutory regime and accompanying judicial construction impose few limits on workplace surveillance of e-mail and Internet use. Nonetheless, employers should avoid the temptation of spying on their employees without notice. Surreptitious monitoring has no deterrent value and breeds resentment and discomfort upon discovery. Instead, each employer should give notice to its workforce of the method and scope of electronic monitoring by promulgating a policy tailored for the employer's particular workplace.