COMPUTER ACCESS:
LIMITATIONS & REMEDIES

PART I

Susan J. Silvernail, Esq.
Marsh, Rickard & Bryan, P.C.
ABICLE 2008 Tort Law Update
December 12, 2008

> It reads like a cold war thriller: The spy follows the suspects through several countries, ending up in Guatemala City, where he takes a room across the hall from his quarry. Finally, after four days of surveillance, including some patient ear-to-the keyhole work, he is able to report back to headquarters that he has the goods on them. They're guilty!
>
> But this isn't a John Le Carre novel, and the powerful institution pulling the strings wasn't the USSR or the CIA. It was Wal-Mart, and the two suspects weren't carrying plans for a shoulder-launched H-bomb. Their crime was "fraternization". One of them, James W. Lynn, a Wal-Mart factory inspection manager, was traveling with a female subordinate, with whom he allegedly enjoyed some intimate moments behind closed doors. At least the company spy reported hearing "moans and sighs" within the woman's room. [1]

The sociologist Barbara Ehrenreich who turned a critical eye toward Wal-Mart's surveillance activities, writes that the cold war thriller analogy is "not entirely fanciful". According to the *New York Times* reporter who first related the story of Wal-Mart's stalking of Lynn and his female colleague, the company's security department is staffed by former top officials of the CIA and the

---

[1] Barbara Ehrenreich, "Wal-Mart and Target Spy on Their Employees", AlterNet, April 6, 2007 (http://www.alternet.org/story/50058/).

FBI. [2]

The relationship between the Wal-Mart executive and his female subordinate was first discovered by Wal-Mart in private e-mails that the company was monitoring. After both employees were sacked, the woman sued Wal-Mart for wrongful termination. The case settled in 2007. The woman's lawyer was interviewed by the National Law Journal. He couldn't discuss the lawsuit owing to a confidentiality agreement. He would only say that "corporate spying in general is a growing widespread practice". [3]

According to the *Wall Street Journal,* Wal-Mart has always placed strict limits on what its employees can do while on the job. [4] For example, the newspaper reports that store employees cannot use personal cell phones on the job. Managers get a list of e-mail addresses and phone numbers their employees have communicated with, and a list of web sites visited. Wal-Mart

---

[2] Barbara Ehrenreich, "Wal-Mart and Target Spy on Their Employees", AlterNet, April 6, 2007 (http://www.alternet.org/story/50058/).

[3] Tresa Baldas, "Companies Keep Watch, Covertly", The National Law Journal, September 2, 2008.

[4] Ann Zimmerman & Gary McWilliams, "Inside Wal-Mart's 'Threat Research' Operation", Wall Street Journal, Page B1, April 4, 2007.

limits internet access, blocking social-networking and video sites. A company spokesperson, Sarah Clark, told the *WSJ* that Wal Mart's security operations are normal: "Like most major corporations, it is our corporate responsibility to have systems in place, including software systems, to monitor threats to our network and our intellectual property so we can protect our sensitive business information". [5]

Is Wal-Mart's surveillance of its employees "normal" as the company claims? While it is likely that Wal-Mart is the extreme –the *WSJ* describes Wal-Mart's team of security professionals dubbed the "Threat Research and Analysis Group" using cutting-edge Department of Defense monitoring systems and working out of a "Bat Cave" [6]--- in most respects, the answer would have to be "yes". According to the American Management Association (AMA) and the ePolicy Institute, who have teamed up since 2001 to survey electronic monitoring and surveillance in the workplace, employers are increasingly combining technology with policy to

---

[5] Ann Zimmerman & Gary McWilliams, "Inside Wal-Mart's Threat Research' Operation", Wall Street Journal, Page B1, April 4, 2007.

[6] *Id.*

manage productivity and protect resources.

According to the 2007 Electronic Monitoring & Surveillance Survey, employers are primarily concerned with inappropriate web surfing, with 66% monitoring internet connections. Fully 65% of companies use software to block connections to inappropriate web sites – a 27% increase since 2001 when AMA/ePolicy Institute first surveyed employers. [7]

Employers who block access to the web are concerned about employees visiting adult sites with sexual, romantic, or pornographic content (96%); game sites (61%); social networking sites (50%); entertainment sites (40%); shopping/auction sites (27%); and sports sites (21%). In addition, companies use URL blocks to stop employees from visiting external blogs (18%). [8]

According to the survey, computer monitoring takes many forms, with 45% of employers tracking content, keystrokes, and

---

[7] AMA/ePolicy Institute, 2007 Electronic Monitoring & Surveillance Report. (In 2007, a total of 304 companies participated: 27% represent companies employing 100 or fewer workers, 101-500 employees (27%), 501-1,000(12%), 1,001-2,500 (12%), 2,501-5,000 (10%) and 5,001 and more (12%)).

[8] AMA/ePolicy Institute, 2007 Electronic Monitoring & Surveillance Report.

time spent at the keyboard. Another 43% store and review computer files. In addition, 12% monitor the blogosphere to see what is being written about the company, and another 10% monitor social networking sites. [9]

Of the 43% of companies that monitor e-mail, 96% track external (incoming and outgoing messages), while only 58% monitor internal messages that are sent among employees. As to monitoring methods, 73% of businesses use technology tools to automatically monitor e-mail, and 40% of employers assign an individual to manually read and review e-mail. Employees assigned to read and review employee e-mail are employed by the following departments: IT (73%), HR (34%), legal (18%), compliance (17%), outside third party (4%), other (17%). [10]

Increasingly, there is teeth in these monitoring policies: more than one-fourth of employers have fired workers for misusing e-mail and nearly one-third have fired employees for misusing the internet. According to the 2007 survey, the 28% of

---

[9] *Id*.

[10] *Id.*

employers who have fired workers for e-mail misuse have done so for the following reasons: violation of any company policy (64%), inappropriate or offensive language (62%): excessive personal use (26%), breach of confidentiality rules (22%), other (12%). The 30% of bosses who have fired workers for internet misuse cite the following reasons: viewing, downloading, or uploading inappropriate offensive content (84%), violation of any company policy (48%), excessive personal use (34%), other (9%). [11]

According to the 2007 Electronic Monitoring & Surveillance Survey, most employers tell their employees that they are being watched. Fully 83% inform workers that the company is monitoring content, keystrokes and time spent at the keyboard, another 84% let employees know the company reviews computer files; and an additional 71% of employers alert employees to e-mail monitoring.

How do the bosses notify employees that they are being watched? In ways that are not necessarily the most effective in

---

[11] *Id*.

the AMA's view: 70% of businesses in 2007 relied on an employee handbook to inform users about computer monitoring; 40% relied on e-mail notices; 35% used written notices; and 32% relied on internet postings. According to the survey, only 27% of employers addressed monitoring policies and practices as part of formal, on-site employee training –the way AMA recommends to maximize compliance. The AMA's position is that formal employee training gives employees the opportunity to ask questions and gain a thorough understanding of electronic rules, policies and procedures. [12]

Nearly half of the employers surveyed by AMA monitor their employees' telephone use: 45% monitor time spent and numbers called, up from 9% in 2001. Another 16% record phone conversations, versus 9% in the first survey. An additional 9% monitor employees' voicemail messages. Most employers notify employees of phone (84%) and voicemail (73%) monitoring. Six per cent of the employers reported that they had fired employees

---

[12] *Id.*

for misuse or private use of office phones. [13]

Almost half (48%) of the companies surveyed use video monitoring to counter theft, violence and sabotage, up from 33% in 2001. Only 7% use video surveillance to track employees' on-the-job performance, a slight increase over the 4% reported in the 2001 survey. Most employers notify employees of anti-theft video surveillance (78%) and performance-related video monitoring (89%). [14]

According to the 2007 Electronic Monitoring & Surveillance Survey, employers have been somewhat slow to adopt emerging technologies to help track employee productivity and movements. Employers who use Assisted Global Positioning or Global Positioning Systems satellite technology are in the minority, with only 8% using GPS to track company vehicles; 3% using GPS to monitor cell phones; and fewer than 1% using GPS to monitor employee ID/Smartcards. The majority (52%) of businesses use Smartcard technology to control physical security

---

[13] *Id*.

[14] *Id*.

and access to buildings and data centers. Very few are using technology yet that enables fingerprint scans (2%), facial recognition (0.4%) and iris scans (0.4%).[15]

> Within its bowels, The Boeing Co. holds volumes of proprietary information deemed so valuable that the company has entire teams dedicated to making sure that private information stays private.
>
> One such team, dubbed "enterprise" investigators, has permission to read the private e-mails of employees, follow them and collect video footage or photos of them. Investigators can also secretly watch employee computer screens in real time and reproduce every keystroke a worker makes...[16]

Boeing was recently the subject of a Seattle Post-Intelligencer investigative story, which questioned its monitoring activities, including the reading of e-mails and the monitoring of employees. Boeing spokesman Tim Neale told the newspaper

---

[15] *Id.*

[16] Andrea James, "Boeing Bosses Spy on Workers", Seattle Post-Intelligencer, November 16, 2007 (http://seattlepi.nwsource.com/business/339881_boeingsurveillance16.html).

that when employees log on to the corporate network they are fully informed that their activities are being monitored. He said only authorized personnel have the capability to monitor corporate systems and they do so only when they have reason to suspect abuse or misuse. "For example, it is against company policy for an employee to use computer systems to run his or her own business", Neal said. "Of course, it is also against company policy to share proprietary information with parties outside the company, unless authorized by management to do so". [17]

The comments suggest much about employers' motivation behind the monitoring and surveillance activities. One lawyer suggests that "on the whole, employers are worried about two key things: their legal liability (which includes exposure to breach of contract, copyright, trade secrets and personal grievances), and loss of productivity or property". [18] This thinking is backed up by the 2007 Electronic Monitoring and Surveillance Survey, which

---

[17] Mel Duvall, "Wal-Mart Spying: Good, Bad or Just the Wave of the Future?", http://www/ciozone.com/index.php/Management/Wal-Mart-Spying-Good-Bad-Or-Just-The-Wave-Of-The-Futureu.html

[18] Anthony Drake, "Employee Surveillance: A New Age in Hi-Tech Spying", Bell/Gully Update, February 2006).

found that employers are spurred by concern over litigation and the role electronic evidence plays in lawsuits and regulatory investigations. Data security and employee productivity concerns also motivate employers to monitor web and e-mail use and content. [19] Employers report an awareness that workers' e-mail and other electronically stored information create written business records that are the electronic equivalent of DNA evidence. Accordingly, 24% of employers have had e-mail subpoenaed by courts and regulators, and another 15% have battled workplace lawsuits triggered by employee e-mail, according to 2006 AMA/epolicy research. [20]

As motivated by litigation as today's businesses may be, the courts have consistently sided with employers when it comes to monitoring and surveillance activities.

One of the most discussed cases in the area of workplace monitoring is *Shoars v. Epson America, Inc*. Like most American companies, Epson had an extensive e-mail system. Alana Shoars

---

[19] *Id*.

[20] AMA/ePolicy Institute, 2006 Workplace E-mail and Instant Messaging Survey Summary.

administered it. When she had trained employees to use the computer system, Shoars had assured them that the company's e-mail system was private and their passwords and communications secure. She discovered it was not. Shoars was instructed to monitor Epson employees' e-mail transmissions. She objected and was fired. Shoars filed suit against Epson in Los Angeles Superior Court in 1990, for wrongful discharge, slander, and invasion of privacy. She argued that California's constitutional protections of privacy should protect her. Epson argued that since the company owned the e-mail system, it had the right to control it and to monitor how it was used. Since the company provided the equipment, the software, and the network, it wanted the right to ensure that its employees used electronic mail strictly for business purposes.

The California Court of Appeal decided there was no California law protecting the privacy of e-mail. The court also rejected Shoars' argument that Epson had violated California's broader constitutional right of privacy. The court ruled that the constitutional right of privacy protected only *personal*

information. The court declined to extend privacy protections to "business-oriented communications". [21]

Bonita Bourke and Rhonda Hall administered an electronic mail system between Nissan and a group of Infiniti dealers in Southern California. They installed hardware and trained the dealers to use the system. Soon the two women began receiving personal messages, some sexually suggestive, over the system. Another Nissan employee spotted such a message and alerted a supervisor. Burke and Hall were warned to curtail the personal e-mail activity, even though they claimed they had not initiated the messages. The women submitted a grievance complaining the company had invaded their privacy by retrieving and reading their e-mail messages. They were soon fired. Bourke and Hall filed suit against Nissan Motor Corporation for common law invasion of privacy and violation of their constitutional right to privacy. Bourke and Hall argued that they had an expectation of privacy because they were given passwords to access the computer system and were told to safeguard their passwords.

---

[21] Charles J. Sykes, "Big Brother in the Workplace", Hoover Digest, No. 3 (2000).

Nissan argued that Bourke and Hall were both aware of the company policy that employees were to restrict their use of company-owned computers to company business. The California Court of Appeal ruled in favor of Nissan, stating "in the absence of a reasonable expectation of privacy, there can be no violation of the right to privacy". [22]

In another key case concerning the privacy of an employee's e-mail, Michael Smyth sent an inappropriate e-mail to his supervisor over the company computer system. The Pillsbury Company's policy was that e-mail communications would remain confidential and privileged. Even more than that, Pillsbury assured its employees, including Smyth, that e-mail communications could not be intercepted and used against its employees as grounds for termination or reprimand. Despite the policy, Smyth was terminated for making inappropriate and unprofessional comments. Smyth sued for violation of his right to privacy. The United States District Court of the Eastern District of Pennsylvania ruled in favor of Pillsbury in 1996. The

---

[22] Bourke, et al, v Nissan Motor Corp., No. B068705 (California Court of Appeal, July 26, 1993).

Court stated, "...[W]e do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management." [23]

As suggested above, federal law does little to restrict employer monitoring and surveillance of its employees. Public employees do enjoy some minimal Fourth Amendment protections against unreasonable search and seizure, but those rights do not extend to the private sector. Congress has not wanted to enact privacy rules for private businesses; in fact, when Congress passed the Electronic and Communications Privacy Act (ECPA) to cover e-mail communication in 1986, it explicitly exempted private employers. [24] "When most Americans go to work in the morning, they might just as well be going to a

---

[23] *Smyth v. The Pillsbury Company,* 914 F. Supp. 97 (U.S. PA. 1996).

[24] The Electronic Communications Privacy Act (ECPA) of 1986: Sets out provisions for access, use, disclosure, interception and privacy protections of electronic communications. The law covers various forms of wire and electronic communications. ECPA prohibits unlawful access and certain disclosures of communication contents. Additionally, the law prevents government entities form requiring disclosure of electronic communications from a provider without proper procedure.

foreign country," says Lewis Maltby of the American Civil Liberties Union Workplace Right Project, "because they are equally beyond the reach of the Constitution in both situations. And unfortunately, federal law does very, very little to fill this void". [25]

CONCLUSION

Research shows that a sizable percentage of businesses monitor their employees' communication activities. When it comes to workplace computer use, employers are primarily concerned about inappropriate web surfing. Most employers notify employees when they are being monitored. New technology tools are increasingly being used to address employers' concerns about the risk of litigation, security breaches and other electronic disasters.

---

[25] Charles J. Sykes, "Big Brother in the Workplace", Hoover Digest, No. 3 (2000).