The Effect of the USA Patriot Act on Workplace Privacy

Clare M. Sproule

The USA Patriot Act has taken the complicated issue of workplace privacy and complicated it further. The wise employer will do well to proceed with caution in all monitoring activities.

AN OFTEN-REPEATED REFRAIN since the terrorist attacks on the World Trade Center and the Pentagon is “How the world has changed since 9/11!” One of the biggest changes, however, may be a shift in employees’ priorities from protecting their privacy towards increasing their security. Prior to the attacks, privacy initiatives were gaining momentum, driven by pressure from legislators, regulators and employee lawsuits. After 9/11, surveillance activities that were objectionable before have suddenly become more palatable when viewed as a response to security concerns both in the workplace and as part of our country’s “Homeland

Clare M. Sproule is a member of the firm of Epstein Becker & Green, P.C., in New York City. This article was originally published in the Cornell Hotel and Restaurant Administration Quarterly, in October 2002, and will be published in the conference volume for New York University 55th Annual Conference on Labor, Workplace Discrimination, Privacy, and Security After 9/11, later this year.
Security” initiatives. Mark G. Young, Note, What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance, 70 Fordham L. Rev. 1017, 1018 n.6 (2001). There is little doubt that privacy will re-emerge as a paramount concern once employees begin to feel more physically secure. Support for all such security measures has waned over time. A week after the attacks, 70 percent of respondents in a poll conducted by Pew Research Center reported that they supported a national ID card that would be shown to authorities on demand. A survey released in March 2002 by Gartner Inc. reported that only 26 percent favored the idea. Julia Scheeres, Support for ID Cards Waning, Wired News March 13, 2002. Employers who develop a monitoring policy now that is sensitive to their employees’ privacy interests, and who communicate the scope and purpose of the monitoring program to their employees, will be ahead when the focus changes from security back to privacy.

PATRIOTS vs. PRIVACY • The real loss of privacy in the workplace since 9/11 will most likely result from the USA Patriot Act, which has the rather cumbersome formal title of “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,” Pub. L. No.107-56, 115 Stat. 272 (2001). The Patriot Act eased the restrictions on the government’s ability to access the electronic information that employers capture and store, rather than from increased employer surveillance.

Monitoring and Security: Questionable Connection

Concern about security is one of the primary reasons given by employers for monitoring the workplace. 2001 AMA Survey, Workplace Monitoring & Surveillance: Policies and Practices, Summary of Key Findings, American Management Association, April 2001. However, when employers refer to security concerns, they are not necessarily referring to their employees’ physical security, which is, of course, the main concern since 9/11. In the January 2001 AMA Survey, employers reported that their main security concern was “protecting the value of proprietary corporate information.” Thirty-seven percent of employers did report, however, that they conducted video surveillance for security purposes, which could be a reference to physical security concerns, but could also be a reference to surveillance to prevent theft of merchandise and/or equipment by employees or others. 2001 AMA Survey, Workplace Monitoring & Surveillance: Summary of Key Findings, American Management Association, January 2001 at p. 1.

Workplace Security: Not Improved

The reality is that the security of most workplaces has not changed as a result of the terrorist attacks. According to an annual survey of Fortune 100 companies conducted by Pinkerton’s, workplace violence and internet/intranet security concerns ranked first and second as the top concerns of corporate managers even before 9/11. See Christopher A. Weals, Workplace Privacy, The Tide Has Turned, Opening the Door to Employers to Snoop—and More., Legal Times, p. S 27, February 4, 2002. In the wake of 9/11, employers are being constantly admonished to improve security in the workplace, even though the threat of a terrorist attack on most workplaces is recognized as being remote. See e.g. American Surveillance and Security, Terrorism in America: What Should Employers be Doing? Florida Employment Law Letter, December 2001. It appears that what is being recommended to employers is to take advantage of the fear engendered by the terrorist attacks and implement tight security and surveillance measures that would have been objectionable before 9/11. See Weals, supra. See also BNA—Employers
Missing the Real Danger: Workplace Violence

The biggest threat to most employees on the job is not terrorism, but rather work-related violence committed by disgruntled fellow employees or ex-employees. The National Institute of Occupational Safety and Health reports that work-related violence is the second-highest cause of death among all male workers in the United States, and the leading cause of death on the job for female workers. Suzanne M. Marsh, Larry A. Layne Fatal Injuries to Civilian Workers in the United States, 1980-1995, DHHS/NIOSH Pub. No. 2001-129S, Table US-7, p. 16, July 2001. However, while much of the electronic information gleaned from employers’ surveillance activities may not be helpful in preventing workplace violence, the government believes such information may be very helpful in preventing future terrorist attacks.

How Far Should Employers Go in Cooperating with Surveillance Initiatives?

One question for employers will be: Should they voluntarily cooperate with law enforcement officials by turning over any such information, or should employees’ privacy interests prevail over the nation’s security concerns? It is reported that increasingly since 9/11 the FBI has been requesting and receiving employee personnel records from employers without a subpoena or warrant. A recent survey by the Privacy Council revealed that since 9/11 airlines, hotels and other travel-related services voluntarily turned over customer and employee information to investigators. See Weals, supra. Since 9/11, the question has been raised about how an employer should react if they come across a controversial e-mail relating, for example, to terrorism or al Qaeda, while monitoring employee communications. Should the company call the police or the FBI? Will it face liability if it does, or if it doesn’t? Id. Employers must exercise caution in this regard since they could be subject to the restraints of the Fourth Amendment if they act as an instrument or agent of the state in effecting a search or seizure. See Young, supra, at 1041 n.115. In light of the Patriot Act, employers may not even be aware of government surveillance of their employees, or may have no choice but to allow the government access to their employees’ private communications. See generally, USA Patriot Act, §§201-25 (amending 18 U.S.C. §§1030, 2510, 2511, 2516, 2520, 2702, 2707, 2711, 2712, 3121, 3123, 3124, 3127, 3103a; 47 U.S.C. §551; 50 U.S.C. §§1803, 1804, 1805, 1823, 1824, 1842, 1843, 1861 et seq.)

EVERYDAY ELECTRONIC MONITORING AND SURVEILLANCE • Even before 9/11, electronic monitoring and surveillance was prevalent in the American workplace. See April 2001 AMA Survey, supra, at p. 4. The AMA offered the following disclaimer: “The original sample of 1,627 mirrored AMA’s corporate membership and client base, who together employ one-fourth of the U.S. workforce, but because such companies are largely drawn from the top five percent of U.S. businesses in terms of annual sales and total employees, that sample did not accurately reflect policies in the U.S. economy as a whole, where smaller firms predominate.” Seventy-seven percent of employers responding to an American Management Association survey in January 2001 reported engaging in some form of electronic oversight of their employees. This number is up from 67 percent who reported doing so just two years earlier. See January 2001 AMA Survey, supra note 4, at p. 1. Active monitoring of employees’ activities has more than doubled since 1997, with the largest increases being in the number of employers re-
Employers responding to the survey reported engaging in some or all of the following forms of monitoring:

- Recording and review of telephone conversations;
- Storage and review of voice mail messages;
- Storage and review of computer files;
- Storage and review of e-mail messages;
- Monitoring Internet connections;
- Video recording of employee job performance;
- Telephone use (time spent, numbers called);
- Computer use (time logged on, keystroke counts, etc.); and,
- Video surveillance for security purposes.

These employers gave five reasons (in order of importance) for monitoring their employees’ activities: legal liability; security concerns (protecting corporate assets); legal compliance; productivity measurement; and performance review. Id.

ELECTRONIC DEVICES: TREASURE TROVES OF INFORMATION • While employers have been recording and storing electronic information on their employees for their own purposes for years, it is doubtful that many of them ever thought that the government would seek to access such information. However, the investigation in the aftermath of 9/11 revealed that the electronic monitoring devices that employers already had in place contain valuable information that the government could use in tracking down and monitoring potential terrorists and their activities. One of the main purposes of the Patriot Act is to make it easier for the government to access and share such information in the interest of preventing future attacks. USA Patriot Act, §203.

The Long Reach of Government Surveillance Techniques

Although the technology used by most employers to monitor their employees has grown more sophisticated over the years, it pales in comparison to the highly sophisticated surveillance devices that the government has at its disposal. While most employers use video cameras, tape recorders and computer programs to monitor and record information, the government uses, among other devices, satellites, wiretaps, microphones, beepers, biometric technology, and a controversial software program called “Carnivore” to conduct its surveillances. For an extremely informative discussion of the covert surveillance technologies used by the government, see Young, supra, at 1023-38. Numerous government agencies use surveillance technologies including the Secret Service, the Central Intelligence Agency, the Federal Bureau of Investigation, the Bureau of Alcohol, Tobacco and Firearms, the Drug Enforcement Agency, the Internal Revenue Service, the Immigration and Naturalization Service, the Environmental Protection Agency and the U.S. Postal Service, among others. Id. at 1040. Distinctions are drawn among the various purposes for which the surveillance is being conducted, whether evidence gathering, general intelligence gathering or intelligence gathering for national security, and different standards apply to each. Id. at 1044. For a listing of the federal laws governing electronic surveillance see Surveillance Laws at http://www.tscm.com/Surveillance_Laws.html.

Ordinary Tools, Extraordinary Information

There are many electronic devices that employers routinely provide to employees for business purposes that employees use for their personal business, with or without their employers’ approval. These devices contain a wealth of information that most employers do not routinely monitor or review, and in some cases, may not