THE EFFECT OF THE USA PATRIOT ACT ON WORKPLACE PRIVACY

By Clare M. Sproule

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 Security” initiatives. There is little doubt that privacy will re-emerge as a paramount concern once employees begin to feel more physically secure. 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.

The real loss of privacy in the workplace since 9/11 will most likely result from the USA Patriot Act, which eased the restrictions on the government’s ability to access the electronic information that employers capture and store, rather than from increased employer surveillance. Even though security concerns is one of the primary reasons given by employers for monitoring the workplace, the reality is, the security of most workplaces has not changed as a result of the terrorist attacks. 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. 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. One question for employers will be – should they voluntarily cooperate with law enforcement officials by turning over any such information, or should their employees’ privacy interests prevail over the nation’s security concerns? 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.

1. **Electronic Monitoring and Surveillance – An Everyday Occurrence**

Even before 9/11, electronic monitoring and surveillance was prevalent in the American workplace. 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% who reported doing so just two years earlier. Active monitoring of employees’ activities has more than doubled since 1997, with the largest increases being in the number of employers reporting reviewing employee computer files and/or e-mail messages. 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,
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.

2. **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.

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. 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. Distinctions are drawn among the various purposes for which the surveillance is being conducted, either evidence gathering, general intelligence gathering or intelligence gathering for national security, and different standards apply to each.

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 even be aware exists. The government, however, has recognized that electronic devices used by employees may contain information associated with terrorist and/or other criminal activity that could be invaluable during an investigation or for intelligence gathering.

Putting aside the invaluable information that can be gleaned from telephone and computer surveillance, according to the U.S. Secret Service, other electronic devices can contain important information as well. Wireless telephones may contain the following useful information: numbers called from the cell phone; numbers saved for speed dial; caller ID for incoming calls to the cell phone; and invaluable information in their memory such as names, addresses, phone and pager numbers, pin numbers and other access numbers and/or passwords. Fax machines can contain speed dial lists, stored incoming and outgoing faxes and fax transmission and receipt logs. Caller ID and electronic paging devices can contain telephone numbers and other alpha or numeric messages. In