Chapter XXII
Electronic Surveillance and Civil Rights

Kevin Curran
University of Ulster, UK

Steven McIntyre
University of Ulster, UK

Hugo Meenan
University of Ulster, UK

Ciaran Heaney
University of Ulster, UK

ABSTRACT

Modern technology is providing unprecedented opportunities for surveillance. Employers can read e-mail, snoop on employee's computer files, and eavesdrop on their calls. Many companies also have cameras monitoring their employees all day. Since employees do not usually have access to their own electronically stored data, they cannot correct inaccurate information. Strangely, this type of information gathering is not illegal even if it is done unbeknownst to an employee. This is because there are no laws regulating electronic surveillance in the private sector workplace. This chapter presents an overview of electronic surveillance and civil liberties.

INTRODUCTION

Employers have a legitimate interest in monitoring work to ensure efficiency and productivity, however electronic surveillance often goes well beyond legitimate management concerns and becomes a tool for spying on employees. In 2002, postal workers in New York City were horrified to discover that management had installed video cameras in the restroom stalls. Female workers at a large north eastern department store discovered a hidden video camera installed in an empty office that was commonly used as a changing room. Waiters in a large Boston hotel were secretly videotaped dressing and undressing in their locker room. Although in each of these instances the employer claimed it was concerned about theft, no illegal acts were ever uncovered. But the employees were robbed of their dignity and personal privacy (ACLU, 2004).

With the amount of information that is freely available on the Internet, people are becoming more informed of what governments, companies, or corporations are doing. The Internet also provides an open forum where citizens can voice concerns for civil liberties (Arterton, 1989). The Civil Liberties Monitoring Project (CLMP)[1] is an American based organisation whose mission statement is to monitor, document, advocate, and educate about civil rights and human rights abuses by law enforcement and other government agencies. The aim of CLMP, founded by local citizens of Southern Humboldt County, CA, is to encourage public awareness of constitutional rights and encourage involvement of the whole community in preserving and protecting these rights. The European equivalent is StateWatch[2] which monitors civil liberties, security, and intelligence issues.

Modern technologies are providing unprecedented opportunities for surveillance. Employers can read e-mail, look at workers computer files and eavesdrop on phone calls. Many companies also have cameras monitoring their employees all day. Since employees do not usually have access to their own electronically stored data, they can not correct inaccurate information. Although it is often done without an employee's knowledge, this kind of information gathering is almost always legal. This is because there are no laws regulating electronic surveillance in the private sector workplace. Employers have a legitimate interest in monitoring work to ensure efficiency and productivity, however it can be argued that electronic surveillance often goes well beyond legitimate management concerns and becomes a tool for spying on employees. Computer data banks help employers track employees' past employment records, financial status, and medical histories. Although there are laws that prevent an employer from sharing intimate employee information with individuals outside the company, there are few restrictions on an employer's right to share it with people on the inside (ACLU, 2004).

We are living in a digital world and surveillance is very much a part of that. It seems that we have to just get used to it. One of the more intrusive mechanisms at present are speed cameras which pick up and record the vehicle registration numbers of any vehicle traveling too fast along particular stretches of road (Simons & Spafford, 2003). They do however often serve another purpose, and that is to identify vehicles without "road tax." This is done by running the plates against a road tax database.

In a security-conscious world it seems that no activity is off limits to government inspection. Polls show that many people are willing to tolerate increased surveillance, higher encryption standards, and other measures for the sake of security (Ang & Nadarajan, 1996; Barquin, LaPorte, & Weitzner, 1995; Borland & Bowman, 2002). But civil libertarians worry that the increased investigative powers granted since the attacks, and people's eagerness to comply with them, have needlessly entangled innocent citizens and threaten to undermine constitutional rights to privacy and free speech. Even without explicit limitations, some say that fear of reprisal may have a chilling effect on public behaviour. Given the proliferation of log files and massive customer databases, combined with easy access to controversial sites and other information, the Internet has accelerated the debate over electronic information and terrorism (Borland & Bowman, 2002). In the United States, since September 11, an unnamed supermarket chain had given shopping club card records to federal investigators and Lexis/Nexis, (the large database containing news articles, legal filings, and public records of all kinds), says it is working more closely with law enforcement on several fronts since September 11, including "authentication" of individuals' identity (Borland & Bowman, 2002).

In early 2005, Google, to the dismay of many, announced that it had agreed to censor its results in China, adhering to the country's free-speech restrictions in return for better access in the Internet's fastest growing market (Liedtke, 2005). Because of government barriers set up to suppress information, Google's China users have been blocked from using the search engine due to barriers or when they can actually get through to the site—they experience long delays in response time. China already has more than 100 million Web surfers and the audience is expected to swell substantially (Liedtke, 2005).