American Journal of Applied Sciences 1 (3): 225-229, 2004
ISSN 1546-9239

Civil Liberties and Computer Monitoring

Kevin Curran, Steven McIntyre,
Hugo Meenan, Francis McCloy and Ciaran Heaney
Internet Technologies Research Group, University of Ulster,
Magee Campus, Northland Road, N. Ireland, BT48 7JL, UK

Abstract: Civil Liberties-the term used for the fundamental liberties and rights of a country's citizen is the right of free speech, thought and action. This is the fundamental building block of a democratic society. This research essay outlines the current measures western governments are taking to ensure our safety and the associated costs of civil and human rights.

Key words: Civil and Human Rights, Countries Citizen, Fundamental Liberties, 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 space 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[1].

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. The Civil Liberties Monitoring Project (CLMP) is an American based organization 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 them. The European equivalent is State Watch which monitors civil liberties, security and intelligence issues.

Modern technologies are providing unprecedented opportunities for surveillance. Employers can read email, look at workers' computer files and eavesdrop on phone calls. Many companies also have cameras monitoring their employees all day. Since employees don't usually have access to their own electronically stored data, they can't correct inaccurate information. Although it's often done without an employee's knowledge, this kind of info-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[1].

We are living in a digital world and surveillance is very much part of that. It seems that we have to just get used to that. One of the most 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. 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 at present, 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[2]. 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 behavior. Given the proliferation of log files and massive customer databases, combined with easy access to controversial sites and other information, the Net has accelerated the debate over electronic information and terrorism[2]. In the United States since September 11th 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 11th, including "authentication" of individuals' identity[2].

Computer monitoring: The Canadian Judicial Council states that "computer monitoring involves the use of software to track computer activities. Monitoring may include tracking of network activities and security threats, as well as Internet usage, data entry, e-mail and other computer use by individual users. Monitoring is done by someone other than the user, and may be made known to the user or may be surreptitious. In either case, the user has no control over the monitoring activities and the data that is generated."

Employers want to be sure their employees are doing a good job, but employees do not want intrusive monitoring techniques used throughout the work day. This is the essential conflict of workplace monitoring. New technologies make it possible for employers to monitor many aspects of their employees' jobs, especially on telephones, computer terminals, through electronic and voice mail and when employees are using the internet. Most people have some form of Internet access at work and a lot of them have some restrictions put on them. These may come in the form of Internet access control developed from packages that were used to restrict children using PCs at home but this has proved difficult to implement and administer, often preventing employees gaining access to legitimate sites; although they have developed new technology that enables greater administration capabilities to be incorporated into applications. Thus different levels of protection can be implemented for different employees. Even with these development companies must trust their employees to use the resource properly. Sometimes this trust can be hard to understand. An employee's productivity, the company's security and liability are all affected by an Internet connection. Take for example some of the figures banded about for the loss of productivity with employees using the Internet during company time. Companies are reported to be losing millions of pounds each year due to employees surfing on the web during working hours. A recent Chartered Institute of Personnel Development (CIPD) report found that UK companies are losing up to £2.5m each year due to non-work-related surfing. Another report claimed that employees posed more problems to businesses than hackers. Viruses can also be downloaded onto their system by the negligence of their employee's. This can happen in a number of different ways. For example an employee may receive a file attachments on a personal Email and when the download it they may not realize that it contains a virus which could cost the company millions if it were to stop operations for any length of time depending on the size of the firm. An employee may take work home with them and work on it on their own PC at home and not realize that they have just brought back in the virus that they did not even realize was on their home computer. Yet again these examples may be accidental but they still cost a lot of money. Email has also made it much easier for information to be passed from one company to another. This in turn makes it much easier for employees to pass information to rival companies as sending attachments by Email is easy to do and with the amount of information that can flow through a company it can be easily missed. This kind of action can be catastrophic for a company such as the case of an employee who came across the plans for a new car design and passed them to a rival which lead to the car design being scraped costing millions. With all these dangers faced by business today people claim that there is no other alternative but to monitor an employee's use of computers[3].

Employees however, are given some protection from computer and other forms of electronic monitoring under certain circumstances. Union contracts, for example, may limit the employer's right to monitor. When using the internet for electronic mail, the employee should assume that these activities are being monitored and are not private. Most people would assume correctly that the company's own e-mail system is being monitored because the employer owns it and I allowed reviewing it. However many employees wrongly believe that by using web based e-mail accounts that these are not being monitored. Indeed, messages sent within the company as well as those that are sent from your terminal to another company or received from another company can be subject to monitoring by employers. Several workplace privacy court cases have been decided in the employer's favor e.g. Bourke v. Nissan, Smyth v. Pillsbury and Shoars v. Epson. Technologies to monitor workplaces have become unavoidable facts of life. A survey by the American Management Association in New York found that 77% of major U.S. firms in 2001 recorded and reviewed employee communications and activities on the job - a figure that had doubled in just four years[4]. More than one-third of companies surveyed said they do video security surveillance and 15 per cent said they keep the tape or digital recordings for review of employee performance. Most of the firms reported they both review and record telephone conversations, voicemail and e-mail messages, and monitor what websites employees go to. Many said they also routinely record the time logged onto a computer and the number of keystrokes people make in a day[4].

Monitoring software and hardware: Keystroke recording software has existed almost since the arrival of the first computers. These programs create a log of all keystrokes typed and store the log file on the computer hard drive. These programs are generally interrupted-driven (from the keyboard interrupt). Thus, it consumes computer time while it reads the keystrokes and writes them to the computer hard drive. Further, the

file on the hard drive may be discovered and erased/ modified. When What Where was one of the first professional monitoring programs available, and has continued to evolve. It can even be set up to automatically uninstall itself at a pre-determined date, possibly preventing detection. Users also have the option of being e-mailed the log files and/or storing them locally on the hard drive. Spector soft can record the screen images, and play them back similar to a VCR. Some programs can email the keystroke logs to a remote computer.

Anti-spy programs can detect and remove software keystroke recorders. *SpyCop* can detect over 300 available keystroke recording programs. SpectorSoft acknowledges that it is detected by the *SpyGuard* antispy software. Some anti-virus programs are also beginning to attack the software keystroke recorders as well. McAfee anti-virus detects some of the popular keystroke recording software. Erasers attempt to cover the tracks of the computer user. Surfsecret Privacy Protector will erase all internet history, and history from over 30 third party applications. Spy Guard combines the anti-spy functions with the eraser functions by both detecting monitoring software and erasing internet history.

Hardware keystroke recorders contain two main components: a simple microprocessor and non-volatile memory. The microprocessor handles tasks such as: interpreting keystrokes, checking for the access password, and displaying menu options. The nonvolatile memory is a fairly large sized memory which is used to store the keystrokes. Non-volatile memory retains data even during a power loss. Hardware keystroke recorders come in two different physical forms. Devices such as 4spycameras keystroke recorders are about the size of an AA battery, and plug into the back of the computer between the keyboard port and the keyboard cable. The InstaGuard computer security keyboard has the hardware keystroke recorder physically built-in to the keyboard case. In both of these cases, the power to the device is supplied by the keyboard port, so that no additional wiring is necessary. Hardware keystroke recorders require no specialized software on the computer system. They are accessed through a "host program", which can be any word processor or text editor. Hardware keystroke recorders are constantly examining the keystroke stream looking for the access password. As soon the device sees the access password, it temporarily shuts down the keyboard and "types" a menu on the screen. This is perhaps the most novel aspect of the hardware keystroke recorder. This technology allows hardware keystroke recorders to be used without installing any software on the computer system, and allows recording to take place without consuming any CPU cycles. Another technology which has governments scared is Pretty Good Privacy (PGP). PGP allows the encryption of information - including electronic mail - with an encryption algorithm that has to date, proven to be unbreakable. This software is so strong that the U.S. Department of Defense has formally declared PGP to be a "munition", and has banned PGP's export outside North America. Some believe that a legitimate use for the above systems might be where a parent or guardian has a serious worry about what their child is viewing or communicating with through the internet.

Governmental surveillance techniques: The European Council has taken steps to establish a Europewide arrest warrant and a common definition of "terrorist crime." Germany's government has loosened restrictions on phone tapping and the monitoring of email and bank records and freed up once-proscribed communication between the police and the secret services. In June 2002, the U.K. attempted to introduce regulations under the pretext of anti-terrorism that would have mandated almost all lo al and national government agencies to gain access without a warrant to communications traffic data. Australia introduced a terrorist law to intercept the email (giving powers to the nation's chief domestic spy agency, the Australian Security Intelligence Organization), creating an offense related to preparing for or planning terrorist acts, and will allow terrorist property to be frozen and seized. New Zealand commenced similar legislation in keeping with the bilateral legal harmonization agreements of the two countries. India also passed its Prevention of Terrorism Ordinance allowing authorities to detain suspects without trial, impose capital punishment in some cases, conduct wiretapping, and seize cash and property from terrorist suspects-despite concerns it would be used to suppress political opponents.

The introduction of compulsory identity cards in Britain has moved a step closer with a plan for "entitlement cards". It is suggested they would be used to clamp down on fraud by checking rights to receive NHS treatment, education and state benefits. The computerized cards could store a photograph, fingerprints and personal information including name and address. David Blunkett has stated that the main use of the cards would be to demonstrate what entitlement people have to state services and not to identify them. David Blunkett states that "We're not interested in just having another form of ID because people already have a passport or driving license"[5]. It is thought the system could also make it easier for banks to cut down on identity fraud, such as credit card crime or bogus benefit claims however Liberty's (a civil liberties organization) campaigns director Mark Littlewood called on the government to look at alternative ways of tackling identity fraud. Rejecting the idea that people would not be forced into carrying the cards, he said: "If it's going to be necessary to have one to access all types of service it is, for all intents and purposes, compulsory"[5].

Since 11 September 2001, some people it seems have become more prepared to give up civil liberties in order to increase security. Not everyone however is convinced that limiting privacy is a good thing. In 2004, US scuba divers found out just how far the long arm of the law can reach since 11 September. Federal agents concerned about scuba-related terrorist plans requested the entire database of the Professional Association of Diving Instructors[2]. Unknown to most of its members, the organization voluntarily handed over a list of more than 100,000 certified divers worldwide, explaining later that it wanted to avoid an FBI subpoena that would have required far more information to be disclosed. Of late, private databases have found their way into the hands of federal investigators hungry for any scraps of data that might serve as leads in terrorism investigations. Grocery shopping lists, travel records and information from other, public databases have all been caught in the government's anti terrorism net[2].

The Federal Bureau of Investigations (FBI) runs an internet surveillance tool called Carnivore, (or DCS1000) which allows law enforcement agents to intercept and collect E-mails and other electronic communications authorized by a court order. Due to the nature of packet networks it is a lot harder to identify particular target information compared with traditional telephone systems. FBI personnel only receive and see the specified communications addressing information associated with a particular criminal subject's service, concerned which a particular court order that has been authorized. Recently, according to an FBI press release the FBI uncovered a plot to break into National Guard armories and to steal the armaments and explosives necessary to simultaneously destroy multiple power transmission facilities in the Southern United States. "After introducing a cooperating witness into the inner circle of this domestic terrorist group, it became clear that many of the communications of the group were occurring via E-mail. As the investigation closed, computer evidence disclosed that the group was downloading information about Ricin, the third most deadly toxin in the world. It is easy to understand why people feel uneasy about Carnivore. The installation of Carnivore of ISP facilities is carried out only by FBI technicians and all the traffic on the ISP goes through the surveillance system which can leave it open to unauthorized surveillance. The system is reportedly able to track a lot more information than it needs which anyone with the correct passwords can access. Compared with traditional wiretapping systems where the provider of the service gathers the information that is required by a court order and hands it over to the agency that requests it, the FBI system can bypass this. This leaves them open to the claim that they break one of the American Amendments that prohibits law enforcement agencies from gathering more information than is required although the bureau says that future systems will have audit trails and features to guard against abuse.

Privacy rights organizations: There are those who oppose the invasion of privacy and fight for the rights of victims of internet abusers. Two of these organizations who oppose privacy invasion are the Privacy Rights Clearinghouse and the Electronic Privacy Information Center (EPIC).

Privacy rights clearinghouse: The Privacy Rights Clearinghouse is a non-profit consumer education and research program which educates on controlling personal information by providing practical tips on privacy protection. The majority of people on a daily basis give away information. "Junk mail" is among the top five consumer complaint topics each year. Wireless phones have become very popular the last number of years and the number of people who use them is steadily growing. Although wireless devices have many advantages, privacy isn't one of them. Depending on the type of phone being used, other people can listen in to conversations. Scanners can zoom in on devices as diverse as baby monitors and walkie-talkies, and can intercept any transmission from emergency and police calls to aircraft to weather reports to user maintenance reports, among others. Wireless phones that operate on a higher frequency (900MHz to 5.8GHz) are more secure but not immune to monitoring. Pager messages are also not immune to monitor, as networks are generally not encrypted. They transmit on lower frequencies that radio scanners and baby monitors, etc. Operate on, although messages cannot be deciphered without special equipment attached to the scanner. It is still unclear on whether text messages, or Short Message Services (SMS) from mobile phones can be intercepted.

A person's chance of landing a job or getting promoted may depend on the information revealed in a background check. Background checks can be random as current employees may be asked to submit a check, but they are often asked from a job applicant. For certain areas of employment, screening is compulsory, for example au pairs and teachers need to have a clean record to stand any chance of a job and employers will scour through their employment history to ensure they have no previous history of ill-treatment of children. In short, employers are being cautious, although applicants and current employees may fear that employers will dig through their history for other reasons than the job. The things an employer needs to know about the applicant can vary with the nature of the job. Negligent hiring lawsuits are rising, and if there is an accident the employer can be liable, which is a good reason to be cautious about potential employees.

Electronic privacy information center: EPIC is a public interest research center, which focuses public attention on emerging civil liberties issues. In January

2004, their Alert newsletter mentioned an agreement between the US and the EU concerning the disclosure of passenger name records of Europeans travelling to the US. The European Parliament criticized this agreement, and urged the European Commission to broker another agreement, which offered genuine privacy guarantees for air passengers. Pending conclusion of this new agreement, the European
The parliament's resolution asked European countries to immediately comply with European and domestic data protection laws. The Spanish government put forward a proposal suggesting airlines which operate within Europe would be required to provide passenger data to governments in the EU country of arrival.

In regards to SPAM, EPIC supports the creation of a Do Not E-mail Registry to prevent spam, which supports enrollment at the domain-level, so that individuals can enjoy whatever benefit it gives without revealing the individuals email address. EPIC also encouraged anti-spam principles endorsed by a coalition of privacy groups, which urged regulators to adopt a clear definition of spam as unsolicited, bulk, commercial mail, to establish opt-in protections, to establish private rights of action for individuals, to enable technical solutions for spam, to support international anti-spam co-operation, and to oppose preemption of state efforts to curb spam.

EPIC and a coalition of privacy and consumer groups have put pressure on Google to suspend its plans to deploy G-mail: a web mail system that will scan users' communications in order to target advertisements. This is regarded as an unprecedented invasion into the privacy of communications. The system keeps communications for an extended period of time, causing users to have less privacy protection in their communications. EPIC launched a page on its site on the privacy of diplomacy in the aftermath of United Nations Secretary Kofi Annan and other UN officials personal conversations' and telephone communications being bugged by the US National Security Agency and the British Government Communication Headquarters[6].

In January 2003, European governments forced Microsoft to modify Passport - an online authentication system which identifies internet users and enables the transfer of personal information between various websites around the world- in order to protect the privacy rights of computer users in the European Union. It was found that Passport violated several EU data protection rules. In stating this rule meant Microsoft had to make more clear privacy rights under European laws and to collect and process personal data fairer. It also gives users the right to indicate on a site by- site basis which personal information they wish to disclose. This rule has waited almost 18 months since EPIC and a coalition of privacy and consumer groups initiated a complaint against Microsoft at the Federal Trade Commission in July 2001, which alleged that Passport violated a section of the Federal Trade Commission Act and constituted an "unfair and deceptive trade practice". EPIC provides an extensive range of secure communications tools on its site such as Crypto Anywhere, Ensuredmail, Hushmail and Mutemail. These tools all basically allow secure e-mail traffic through encrypted connections.

CONCLUSION

Governments are seeking to control the internet and monitor computers because of the current threat of terrorism. In the US, the Patriot Act has been introduced. This brings into question civil liberties of privacy versus security for a government or employer or indeed another individual[7].

Indeed, the current trend of information gathering is growing and without proper restrictions leaving it open to abuse and mishandling. The freedom of information act entitles us to know exactly what information is being held for us by businesses and even the police. There is a very small amount of people who actually know this or who take of advantage of this opportunity. There is always a chance that incorrect information gathered about us is being used in decisions that affect us adversely in the future. Simon Davies[8] sums this topic up and splits the beliefs of citizens into just two groups. "A sceptic would call this censorship; a patriot would call it cooperation." This is true to a certain extent but it is in everyone's interest to ask the difficult questions of our governments and to preserve our civil liberties today, but for the future generations.

REFERENCES

1. American Civil Liberties Union. Privacy in America – Electronic Monitoring. http://archive.aclu.org/library/pbr2.html
2. Borland, John and Bowman, Lisa. 2002. Terrorism. Liberty vs. Security, ZDNet.com, August 27, http://zdnet.com.com/2100-1105-955493.html
3. Lucas D. Introna. 2000. Workplace Surveillance, Privacy and Distributive Justice. ACM SIGCAS Computers and Society, 30: 33-39.
4. Immen, Wallace, 2004. Workplace privacy gets day in court. The Globe and Mail, Wednesday, April 28, http://www.theglobeandmail.com
5. BBC News Online, 2002. Move towards compulsory ID cards, 5th February, http://news.bbc.co.uk/1/hi/uk_politics/1802847.stm (Accessed 25/5/2004)
6. BBC News, 2004. UN bugging scandal widens .27th February. http://news.bbc.co.uk/2/hi/asiaacific/ 3492146.stm
7. Ministry of Research. The Global Short-Circuit and the Explosion of Information, 1996. http://www.fsk.dk/fsk/publ/info 2000-UK/chap01.html
8. Simon Davies, 2002. A year after 9/11. Where are we now? Communications of the ACM, 45: 35-39.