




Monitoring and Surveillance in the Workplace: Lessons Learnt? – Investigating the International Legal Position

Verine Etsebeth

University of Johannesburg, South Africa, vetsebeth@uj.ac.za

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Scholarly Commons Citation

Etsebeth, Verine, "Monitoring and Surveillance in the Workplace: Lessons Learnt? – Investigating the International Legal Position" (2007). *Annual ADFSL Conference on Digital Forensics, Security and Law. 2.* <https://commons.erau.edu/adfsl/2007/session-5/2>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



Monitoring and Surveillance in the Workplace: Lessons Learnt? – Investigating the International Legal Position

Verine Etsebeth
University of Johannesburg
South Africa
vetsebeth@uj.ac.za

ABSTRACT

When considering the legal implications of monitoring and surveillance in the workplace, the question may be asked why companies deploy computer surveillance and monitoring in the first place. Several reasons may be put forward to justify why more than 80% of all major American firms monitor employee e-mails and Internet usage. However, what most companies forget is the fact that the absence or presence of monitoring and surveillance activities in a company holds serious legal consequences for companies. From the discussion in this paper it will become apparent that there is a vast difference in how most countries approach this subject matter. On the one hand America does not afford any employee a reasonable expectation of privacy when it comes to the use of corporate computer resources and systems, while in contrast to this position the United Kingdom goes out of its way to protect each employee's reasonable expectation of privacy. This paper will not only investigate the different approaches followed by some of the world-leader, but will also investigate the legal consequences embedded in each approach. This paper will ultimately enable the reader to judge for himself/herself which approach his/her country should follow while being fully informed of the legal consequences attached to the chosen approach.

Keywords: information security, legal issues, monitoring and surveillance, privacy

1. INTRODUCTION

There are various legal issues that are embedded in workplace monitoring and surveillance. Mainly, there are two main schools of thought that exist on this subject-matter. On the one hand there are those that argue that employers are the owners of the computing equipment, resources and systems and they therefore have a right to monitor how their property is being used, and then there are those that argue that employees' rights to privacy should weigh more than that of any employer.

When examining the relevant statutes, case law and regulations it becomes apparent that in most jurisdictions a notice requirement exist, but this notice of surveillance and/or monitoring is rarely sufficient. This paper will examine Internet and e-mail related surveillance and monitoring in the workplace from a comparative legal perspective. Ultimately, the aim of this paper is to inform readers of the current legal position existing in some of the most important jurisdictions world-wide, thereby enabling readers to make up their own minds on which approach their country should follow, and enabling readers to understand the legal consequences embedded in each approach.

2. JUSTIFICATION FOR MONITORING AND SURVEILLANCE IN THE WORKPLACE

“Surveillance technology is neither inherently bad nor good, but ...there is both good and bad surveillance.”

When considering the legal implications of monitoring and surveillance in the workplace, the question may be asked why companies deploy computer surveillance and monitoring in the first place. Several reasons may be put forward to justify why more than 80% of all major American firms monitor employee e-mails and Internet usage. The first reason centers around employee productivity. As a result of the Internet and e-mails employee productivity has decreased. This is a major concern for employers, as Internet use surveys continue to indicate that the majority of employees spend anywhere

from 10 minutes to an hour every day surfing sites unrelated to doing their jobs – using their work computers to read virtual newspapers, or go online shopping, or even viewing naked woman. Secondly, network performance must be considered. Employees that download video or audio files from the Internet are taking up a great amount of bandwidth. It therefore makes sense that employers spend money on Internet monitoring tools rather than on increasing the bandwidth. Thirdly, the very real risk exists that a company may be held legally liable for the online activities performed by its employees. For example the brokerage firm of Morgan Stanley was exposed to \$70 million lawsuit because of racist jokes that appeared on the company's e-mail system. Also, Dow Chemicals discovered through computer surveillance technologies that 50 employees were using the company's computers to store and send sexual or violent images, resulting in the termination of all of these employees. Fourthly, all companies are faced with the ever present 'insider threat'. It is therefore understandable that companies will go to great lengths to protect the confidentiality of its corporate information and trade secrets even if it is from its own employees.

3. MONITORING AND SURVEILLANCE – THE CANADIAN PERSPECTIVE

3.1 Introduction

It is generally accepted that in terms of Canadian law employees enjoy very little to no privacy protection in the workplace when it comes to computer and email surveillance. MacIsaac observes: "...many employers consider electronic mail sent and received using company computer equipment and stored on company computer networks to be the property of the employer. From the employer's perspective this is a business resource paid for by the employer and is to be used only for business purposes. Therefore, e-mail messages and telephone conversations made on behalf of the employee in the course of business should be made available for review for legitimate business and security reasons. For these reasons, an employee acting on behalf of their employer should have no reasonable expectation of privacy".

This view was supported in an arbitration case in which a college lab technician's employment was terminated after sending unwarranted allegation against other employees to the campus-wide email message board. The case finding reiterated the principle of 'office e-mail: no reasonable expectation of privacy'.

Today however, a definite move towards finding a balance between monitoring and privacy may be observed in Canadian law. As stated in the previous chapter, the most important source of privacy protection in Canada is found in the Personal Information Protection and Electronic Documents Act (PIPEDA) 2000. PIPEDA recognizes the importance of finding a balance between an employer's need to collect certain personal data, and an employee's need for privacy protection. The Act states: "...the purpose of this part [Protection of Personal Information in the Private Sector] is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the rights to privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances".

3.2 Regulatory framework – PIPEDA

When evaluating employee surveillance within the ambit of PIPEDA the following observations should be made:

- (i) Firstly, the provision in PIPEDA of 'appropriate purpose' limits the use, collection and disclosure of personal information to situations which a reasonable person would deem to be appropriate under the circumstances. Within the ambit of the workplace this would imply that mere consent by an employee to surveillance is no longer sufficient as the provision clearly states that a reasonable person must consider the circumstances to be

appropriate. Therefore it may be argued that where surveillance takes place under the façade of creating and maintaining a harassment free and safe working environment, it is likely that the courts will declare such surveillance to be unlawful because of the absence of a known issue in response to which surveillance takes place;

- (ii) Secondly, PIPEDA requires of companies must appoint a privacy officer who will be responsible for ensuring that the company complies with its privacy obligations. The act suggests that the collection of personal workplace data no longer falls within the exclusive jurisdiction of the company's technology personnel, but the privacy officer must also be involved;
- (iii) Thirdly, the act contains specific provision relating to the notification of employees of workplace surveillance. It is expected of companies to: (a) identify the purpose for which the data is being collected; (b) obtain consent prior to collection; and (c) to limit collection of personal data to that which is necessary for the purposes as set out by the company. The aim of these provisions are to: (a) limit the type of information a company may collect; and (b) demand of companies to inform their employees of the surveillance policies of the company. The act does however contain an exception to the general rule that notice must be given to employees before surveillance may take place. Section 7(1) (b) of the act states: "...an organization may collect personal information without the knowledge or consent of the individual only if ...it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of laws of Canada or a province".
- (iv) Fourthly, the Act requires that "personal information shall be retained only as long as is necessary for the fulfillment of the [identified] purpose". Therefore, this provision regulates an employers' use of information after collection thereof. Employers are furthermore prohibited from keeping personal information for an unlimited time period.

3.3 Employee monitoring and surveillance – The present position in Canada

The Canadian court's commitment to privacy protection has come to the fore in recent years. In 1999 the B.C. Supreme Court ruled in the Weir case that e-mail does enjoy a reasonable expectation of privacy. Also in that same year the case of *Pacific Northwest Herb Corp v Thompson* 1999 BCJ No 2772 came before the court. Thompson was an employee of Pacific Northwest who used the company's computer in his home for business and personal purposes. After termination of his employment he continued using the company computer for personal purposes. Amongst the documents on the computer was a file containing documents relating to the wrongful dismissal action he was planning to institute against Pacific Northwest. Before returning the computer to the company he hired a computer consultant to erase all the data on the hard drive. His attempts were however unsuccessful, and after returning the computer to Pacific Northwest the company was able to restore the data. Thompson sought an interdict to prevent Pacific Northwest to exploit the data, claiming that his right to privacy and solicitor-client privilege has been infringed. The judge in this case concluded that Thompson had a reasonable expectation of privacy regarding documents that were created for personal use.

In *R v Duarte* 1990 1 SCR 945 the judge concluded that although the right to privacy was not absolute, it must be "judged against what is reasonable in the circumstances and, amongst other things, is dependant upon competing interests such as the relationship between the parties". The court went even further and stated that in order to determine what would amount to 'reasonable in the circumstances', three considerations must be kept in mind: (i) whether it was reasonable to request surveillance; (ii) whether the surveillance was conducted in a reasonable manner; and (iii) whether any other alternatives to surveillance were available to the employer.

This case has been approved in many other cases. In *St Mary's Hospital and HEU 64 LAC (4th) 382* an electrician discovered a video camera in the ceiling of a manager's office. The local union was outraged at this surreptitious surveillance, and filed a grievance. The arbitrator found in this case that surveillance can be characterized in three ways: (a) benign surveillance which would entail surveillance done for the benefit of the employee; (b) security surveillance which has as its main aim to ensure the protection of employees as well as the employer; and (c) surreptitious surveillance which represents the most intrusive force of surveillance. The arbitrator was of the opinion that this form of surveillance requires strict justification. Furthermore, in *Re Toronto Transit Commission and ATU Loc 113 (Belsito) 95 LAC (4th) 402* and in *New Flyer Industries Ltd and CAW Canada Loc 3003 (Mogg) 85 LAC (4th) 304* the court acknowledged that "surveillance by an employer may, in certain circumstances, infringe upon an employee's right to privacy to an unreasonable extent".

The Privacy Commissioner has made his views on workplace surveillance, the privacy of e-mails and the reasonable expectation of privacy clear. The Commissioner states: "I don't accept that the protection necessarily translates into wholesale surveillance of e-mails or computer use. We accept that there are stringent limits on an employer's rights to read employees' mail, eavesdrop on their telephone calls or rifle through their desk drawers. I think we have to look closely at e-mail communications to see what principles should apply there as well".

The Commissioner went on to comment on the practice of some companies to state in their email policies that the employees should have no reasonable expectation of privacy when using the e-mail systems: "[t]he law of privacy has developed around the notion of the 'reasonable expectation'; one of the ways that the courts determine whether privacy has been violated has been to determine first whether a person could have reasonable expected privacy in a particular place and time. But I don't agree that it follows that an employee's or anyone's privacy can be simply eradicated by telling them not to expect any. While management has the right and the responsibility to manage, it has to operate within limits, including respect for fundamental rights. It is not for management alone to determine whether an expectation of privacy is reasonable".

Therefore, a clear shift in the pendulum in Canadian law may be observed. In the past emphasis was placed on whether or not the employee had a reasonable expectation of privacy, today emphasis is placed on the question whether or not the surveillance is reasonable. It is now accepted that workplace surveillance, whether it be by video camera, server-side computer monitoring, or client-side computer monitoring, cannot be justified by simply giving notice to an employee. An investigation will have to be launched into the reasonableness of the surveillance.

Geist identifies six factors which may be taken into consideration when wanting to determine whether or not the computer or email surveillance is reasonable in terms of Canadian law:

- (i) The target of the surveillance – Consideration must be given to whether computer surveillance will be conducted across the company as a whole or if it will be targeted against specific employees;
- (ii) Purpose of the surveillance – Companies that install new surveillance technologies must be able to show how these technologies support their objectives;
- (iii) Alternatives to surveillance – It is suggested that other surveillance technologies that are much less intrusive on an employee's right to privacy in the workplace must first be investigated;
- (iv) The surveillance technology – The choice of surveillance technology must be reasonable taking into account the purpose of the surveillance;
- (v) Adequacy of notice – in terms of the Criminal Code as well as PIPEDA consent must be obtained from the employee. This would entail not merely informing employees of the

fact of surveillance but also giving them an accurate description of the company's surveillance practices; and

- (vi) The implementation of the surveillance activities – the company will have to ensure that unauthorized persons are not able to gain access to the surveillance information.

3.4 Conclusion

From the above it may be concluded that in Canadian law neither the right to privacy nor the right to surveillance is absolute. Canadian law attempts to find a balance between the interest of the employer and the rights of the employee by focusing on the reasonableness of the surveillance.

4. MONITORING AND SURVEILLANCE IN THE WORKPLACE – THE AMERICAN POSITION

4.1 Introduction

At present the position in America is that no employee has any constitutional, federal or common law legal remedies for redress where an employer abuses email and Internet monitoring and surveillance.

4.2 Constitutional protection against employee monitoring and surveillance

▪ Federal constitution

The US Constitution does not afford anyone the right to privacy expressly. The constitution only recognizes privacy as a penumbral theory. This explains why the right to privacy has not been extended to protect an employee's electronic communications. Cherminisky observes: “[m]ost Americans would be surprised to learn that there is no right to privacy granted in the United States Constitution. The Fourth Amendment protects privacy in limiting police searches and arrests, but privacy in terms of autonomy and the right to be left alone by the government is not mentioned in the text of the Constitution”.

Consequently, the present position in the United States is that employees, in a private workplace, are not afforded any protection against electronic surveillance because of the doctrine of state surveillance. In contrast to this public sector employees have a certain degree of constitutional protection against abusive monitoring in the workplace. Included in this would be the right to reasonable searches and seizures. American courts have even gone so far as to state that public sector employees have a reasonable expectation of privacy regarding their emails and Internet communications.

▪ State constitution

Privacy protection in respect of state constitutions vary to a great extent. It is however important to bear in mind that to date no court has extended state constitutional protection of privacy to email monitoring and surveillance in the workplace. Most states do not require employers to give employees any form of notification when monitoring their emails and Internet communications.

4.3 Federal legislation – The ECPA

▪ Title I of the ECPA – The Federal Wiretap Statute

In terms Title I (The federal Wiretap Act) of the ECPA interception of electronic communications such as telephone calls and emails are prohibited. The Act prohibits the following activities:

- (i) intercepting or endeavoring to intercept electronic communications;
- (ii) disclosing or endeavoring to disclose intercepted electronic communications; and
- (iii) using the content of intercepted information.

It therefore follows that if an employer intercepts email or monitors Internet communications of his/her employee, his actions will fall within the ambit of the ECPA. The following important

observations must be, made in this regard. First, it is required that the interception and/or monitoring should be made intentional. Secondly, the content of the communication is only protected as long as it is under transmission. Consequently, Title I will not be applicable where an employer searches an employee's stored emails.

Two exceptions are contained in Title I. First, the ECPA allows service providers to intercept and disclose electronic communication if either the sender or the receiver consented thereto, or the 'ordinary course of business' exception can be applied. The latter exception however, proves to be highly problematic.

In order for an employer to make use of the 'ordinary course of business exception' it is expected of the employer to prove the following:

- (i) the device used to intercept the electronic communication is "a telephone or telegraphic instrument, equipment or facility, or a...component thereof," provided or installed by the employer himself/herself; and
- (ii) that the specific device is employed by the employer in his/her ordinary course of business.

It must furthermore be borne in mind that an employer is only authorized to intercept the communication for long enough to determine the nature of the conversation. Once the employer has determined that the communication is personal in nature he/she must immediately terminate interception.

▪ **Title II of the ECPA – The Stored Communications Act of 2005**

Title II of the ECPA (The Stored Communications Act of 2005) provides guidance when wanting to obtain access or disclosure of electronic communication, such as messages left on a voice machine, once in storage. A violation of Title II will result in civil liability for any person who (a) intentionally accesses, without authorization, a facility through which an electronic communication service is provided; or (b) intentionally exceeds an authorization access and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage.

As soon as an electronic message has been stored the SCA will regulate the situation. This is irrespective of the length of storage.

When considering the operation of Title II it becomes evident that emails are generally considered to be stored communications in terms of American law. Consequently, employers are authorized to access electronic communications under this title. However, this means that Title I of the ECPA is in actual fact rendered useless.

From the above discussion it may be concluded that in virtually all cases decided by American courts in the last decade it has been decided that employees do not have a reasonable expectation of privacy. In some instances American courts have gone so far as to validate employee monitoring even where advance warning was not given to the employee. The following American case law supports this statement:

▪ **Employee monitoring and surveillance without notice**

In *Restuccia v Burk Technology* 1996 Mass Super LEXIS 367 (Super Ct (Mass) Aug 13 1996) the employer neglected to have an email policy stating the possibility that emails can be monitored, stored on back-up or that emails may not be used for personal messages. When viewing back-up files the employer discovered email messages containing nick-names for the president of the company and references to an extra-marital affair with another employee. The president of the company terminated the two employees' employment based on the fact that they were using the email system too much. The ex-employees argued that they had a reasonable expectation of privacy because of the fact that they had personal passwords to access their message system. The court found that the president's action

of reading the email messages on the back-up system constituted an infringement of the privacy of the ex employees. In this case the ex-employees were successful in their claim, but in every other workplace interception case the defendant's were awarded summary judgment in a claim that workplace surveillance invaded a plaintiff's right of privacy.

Furthermore, in *Smyth v Pillsbury Co* 914 F Supp 97 (ED Pa 1996) an employee was fired after having made negative comments about a sales manager in an email. The email contained treats to "kill the backstabbing bastards". The company had, on various occasions, assured its employees that all emails are confidential and privileged. The company based the termination of employment on "transmitting what it deemed to be inappropriate and unprofessional comments over the company's e-mail system". The employee however argued wrongful termination. The federal court decided that the termination of the employee was justified, as the employee had no expectation of privacy in the employer's email system. The court went even further to state that even if the employee had a reasonable expectation of privacy it would not amount to invasion of privacy if an employer intercepted messages on a system it owned.

Moreover, in *McLaren v Microsoft Corp* Microsoft 1999 Tex. App. LEXIS 4103, 1999 WL 339015 (Tex. Ct. App. 1999) accessed personal folders on a network in order to investigate claims of sexual harassment. The employee claimed that Microsoft had violated his reasonable expectation of privacy. The emails that Microsoft eventually uncovered did provide evidence that the employee was engaging in a "systematic pattern of sexual harassment". The court held that it was not going to recognise a cause of action for invasion of privacy, even though the employee had a special password and the files were marked 'personal'. The court stated in this case that the decisive factor was that the computer was the property of the employer and formed part of the computer environment. The court furthermore stated that because of the fact that the folder was transmitted over the network, it was inevitable that it would be accessed by a third party at some stage. Consequently, the plaintiff had no expectation of privacy with regards to the files marked 'private'.

▪ **Employee monitoring and surveillance with notice**

By implementing an email and Internet policy companies safeguard themselves against any privacy-based claims by employees. In *Bourke v Nissan Motor Corp* Nissan California Court of Appeals, Second Appellate District, Case No. B068705 (July 1996) made every employee sign a waiver form in which they had to acknowledge that they understood that Nissan's email system was to be used for business purposes exclusively. In this case the court decided that this waiver was fatal to any claim an employee can bring based on invasion of privacy.

Furthermore, in *Garrity v John Hancock Mutual Life Insurance Company* 2002 US Dist. LEXIS 8343 (D Mass. May 7, 2000) two long term employees forwarded sexually explicit jokes to third parties. One of their co-workers complaint after receiving such an email. The company had an email policy providing that "messages that are defamatory, abusive, obscene, profane, sexually orientated, threatening or racially offensive" are prohibited. The two woman's employment was consequently terminated. The court dismissed the privacy based action brought by the two women stating that employees do not have any reasonable expectation of privacy pertaining to work related emails. The court furthermore made a very harsh statement by stating that the fact that the company had an email policy was irrelevant. The court concluded that the employer's right and duty to limit harassment in the workplace outweighs any rights the plaintiffs' though they had in respect of privacy.

Moreover, in *Thygeson v US Bancorp* 2004 US Dist. LEXIS 18863 (D. Ore. Sept 15, 2004) the bank's employment handbook stated that employees were prohibited to "use US Bancorp computer resources for personal business". The handbook furthermore stated "do not access inappropriate internet sites and do not send emails which may be perceived as offensive, intimidating, or hostile or that are in violation of Company policy". One of Bancorp's employees were spending more than four hours a day visiting non work related Internet sites on his work computer. The company furthermore discovered

that he was viewing “inappropriate emails containing pictures of nudity and sexually offensive jokes”. The employee was subsequently fired. The employee brought an action against the bank arguing that they invaded his privacy as well as the federal Employee Retirement Income Security Act (ERISA) by firing him without awarding him severance pay. The court found that the employee had no expectation of privacy when his employer accessed the files on its network that the plaintiff saved using a personal password, then this employee had no expectation of privacy in his email ‘merely labeled personal’ without even creating a password.

4.4 Conclusion

The conclusion must be reached that when it comes the subject matter of workplace monitoring and surveillance, all indication are that it is pro-employer. Employees have no real remedies for the abuse of email and Internet monitoring and surveillance. Furthermore almost all courts in America have held that employees do not have a right to privacy in the workplace. Courts continue to justify their position by stating that since business computers are the property of its employers, employers have an unfettered right to monitor its usage. American employees will furthermore be unable to find any relief in the US constitution, common law of torts or the ECPA.

5. MONITORING AND SURVEILLANCE IN THE WORKPLACE – THE UNITED KINGDOM’S PERSPECTIVE

5.1 Introduction

The United Kingdom is a member of the European Union. Consequently, the United Kingdom has to comply with EU directives on the subject matter of employee monitoring and surveillance. In terms of the European Community Treaty it is expected of the UK to propagate enabling legislation which will give effect to the fundamental rights as set forth in the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (ECHR) and legislation of the EU.

5.2 Regulatory framework

Because of the operation of the doctrine of vicarious liability, the UK government has accepted that employers do have the right to monitor their employees. However, in contrast to the approach followed in America, the right of an employer to monitor is balanced with the employee’s right to privacy.

The legal framework for Internet monitoring in the United Kingdom comprises of five main statutes and almost no case law on the subject matter.

▪ The Data Protection Act of 1998

All British employers must comply with the United Kingdom’s implementation of the European Union Directive on Data Protection in the form of the Data Protection Act of 1998. In terms of the DPA data controllers are compelled not only to inform the employee of the monitoring system, but also to protect the data processed in accordance with the Data Protection Principles (DPA).

In terms of the DPA electronic monitoring has to comply with the following requirements:

- (i) the monitoring must be lawful and fair;
- (ii) the monitoring program must be necessary; and
- (iii) the monitoring program must be proportionate to achieving the legitimate business objective while simultaneously protecting the right to privacy of the individual employee.

In terms of the DPA only one exception exists regarding the notification requirement: if electronic monitoring is done with the aim of preventing a specific crime the employer will not have to adhere to the notice requirement.

▪ **The Human Rights Act of 1998**

The DPA furthermore takes cognizance of the Human Rights Act of 1998. In terms of this Act the privacy of any private communication, telephone conversation and email communication is expressly protected. It is important to observe that the Human Rights Act draws a distinction between public and private sector employers. If the employer falls within the ambit of the public sector, the employee will have a direct cause of action in terms of the Human Rights Act.

Employees in the United Kingdom enjoy further protection in terms of article 8 of the ECHR. In terms of article 8 of the Act “everyone has the right to respect for his private and family life, his home, and his correspondence”. This convention affords private employees with a legal remedy to challenge abusive monitoring practices. The European Court of Human Rights has extended the definition of ‘private life and correspondence’ to include business relations, emails and other electronic communications.

Furthermore, the United Kingdom’s chief regulatory agency (OFTEL) issued in 1999 Guidance on recording on private conversations. The aim of these guidelines was to provide employers with guidelines when wanting to implement electronic monitoring without violating their employees’ right to privacy.

▪ **The Regulation of Investigative Powers Act of 2000**

In terms of this Act it is a criminal offence to intercept data without authorization. It is however important to keep in mind that RIP is not applicable to private telecommunications systems such as intranets and Virtual Private Networks. Moreover, no provision in RIP addresses electronic monitoring in the workplace expressly. In general employers are permitted to intercept emails and to monitor Internet access as long as both the sender and receiver agree thereto. Employers may furthermore only intercept emails and Internet communications if the monitoring is conducted in order to carry out the employer’s business activities.

▪ **The Lawful Business Practice Regulations (LBPR)**

This Act governs the rights and responsibilities of businesses relating to monitoring electronic communications. This Act provides certain exceptions to the RIP Act. The most important of which is that monitoring without compliance with the notice requirement can take place. In terms of this exception companies may monitor and keep record of Internet communications in order to comply and adhere to regulatory or self-regulatory practices and procedures. There is however a limitation placed on monitoring activities by providing that such activities may only take place if a company employee uses the computer system within the scope of his/her duties. Furthermore, in terms of the LBPR interception without consent is authorized if the interception has one or more of the following purposes:

- (i) to establish the existence of facts, to ascertain compliance with the regulatory or self-regulatory practices or procedures (quality control and training);
- (ii) to prevent or detect crimes;
- (iii) to investigate or detect unauthorized use of telecommunication systems;
- (iv) to secure; and
- (v) to determine whether or not the communications are business communications.

It should furthermore be kept in mind that interception will only be authorised if the controller of the telecommunication system (employer) made reasonable efforts to inform potential users that interception may take place. Also the scope of application of this Act is limited to business communication therefore the interception of personal communications will not be legal in terms of this act.

5.3 Conclusion

In terms of the RIP Act, LBPR and the DPA it would appear that an employer will only be authorized to lawful intercept communications if it is done 'in the course of transmission'. The legislature therefore encourages UK companies to have a clearly Internet and email usage policy in place. If an employee wants to base his/her claim on infringement of privacy, the Code of Practice will be the most effective regulation for him/her to rely on.

6. CONCLUSION

It is evident from the preceding discussion that Canada, the United States and the United Kingdom have very different views on the protection that should be afforded to employees when dealing with monitoring and surveillance in the workplace.

In America a pro-employer regime is applied in terms of which employees have lost all their privacy based actions. Consequently, employees in America have no reasonable expectation of privacy. It would appear as if American employers have an absolute immunity against the constitution, common law and federal statutory remedies for abusive surveillance practices. In terms of American law it is evident that everything including electronic communications on a work computer belongs to the employer. Furthermore, business and private communications are deemed to be the property of the employer. Therefore, employers are permitted to monitor any electronic communication even if the employer has no e-mail and/or Internet usage policy in place which could serve to notify employees of the fact that their electronic communications are being monitored.

In stark contrast to the American position, in the UK the monitoring and surveillance of employees are strictly proscribed. In the EU and consequently in the UK, electronic monitoring must be reasonably based, proportional, transparent and non-discriminatory. The European Court of Justice feels that it is very important for companies to have written e-mail and Internet usage policies stating what the company's position is regarding employee surveillance and monitoring. This is in contrast with the position in America where courts have allowed the surveillance of emails even in situations where the company guaranteed its employees privilege and confidentiality.

The Canadian position relating to employee monitoring and surveillance fits in comfortably somewhere between the UK and the USA. Although this country have enacted legislation regulating employee monitoring and surveillance, with a built-in notification requirements. The biggest deficiencies encountered in these statutes are that they only contain a notification requirement and not a consent requirement.

The question may be asked which approach is correct? Although from a legal perspective most academics would insist that the United Kingdom's approach is correct, the writer is of the opinion that the current political and social climate must play a very important role in deciding which approach a country should take to this subject matter. Moreover, when considering the fact that a company can incur legal liability for the illegal and inappropriate acts performed by its employees when making use of the corporate computer resources and systems, the writer feels that an employer should have the right to monitor e-mail and Internet usage without too many restraints being placed on him/her. Therefore, the writer is in favor of the American position pertaining to this subject matter. Perhaps countries such as the United Kingdom and Canada should rather ask themselves if they are not empowering employees too much, because at the end of the day, it is still the employer's computer resources and systems that are being used, so why should an employer not be afforded the right to protect its own assets through monitoring and surveillance, especially when considering the fact that an employer can be faced with numerous lawsuit based on the inappropriate use of its computer assets and resources?

7. REFERENCES

Journals

- Blackman and Franklin (Aug 1993) "Blocking big brother: proposed law limits employer's right to snoop" *NYLJ* 5
- Ciocchetti (2001) "Monitoring employee e-mail efficiency workplace vs employee privacy" *Duke Law & Technology* 0026 6
- Greenberg "Comment, e-mail and voice mail: employee privacy and the federal Wiretap statute" *American University Law Review* 22 219, 247-48
- Harnden "Office e-mail: no reasonable expectation of privacy" *FOCUS: Employment Law* No 3 7
- Newton "Proposed NSW workplace surveillance bill extends employees' protection from surveillance in the workplace" (2004) *Workplace and Employee Relations Law Update*
- Sneddon and Troiana "New tort of invasion of privacy and the Internet" (2003) *Internet Law Bulletin* 6(6) 1
- Wilborn, S.E. (1998) "Revising the public/private distinction: employee monitoring in the workplace" *Ga L Rev* 32 825
- Chemirinsky, E. (2003) "Privacy and the Alaska Constitution: failing to fulfill the promise" *Alaska Law Review* 20 29

4

Websites

- American Management Association (2004) "More companies watching employees, American Management Association survey reports"
<http://www.amanet.org/press/amanews/ems2001.htm> (5 May 2004)
- Chen, H. (2004) "Internet use survey 2000 – Trends and surprises in workplace web use"
http://vualt.com/nr/main_article_detail.jsp?article_id=19331 (4 June 2004)
- Federal Privacy Commissioner (2004) "Annual report 2000-2001"
http://www.privcom.gc.ca/information/ar/02_04_09_e.asp (4 January 2004)
- Geist, M. (2005) "Computer and e-mail workplace surveillance in Canada: the shift from reasonable expectation of privacy to reasonable surveillance"
<http://www.michaelgeist.ca/content/94/163> (5 May 2005)
- Hawkins (2004) "Who's watching now? Hassled by lawsuits, firms probe worker's privacy"
<http://www.usnews.com/usnews/nycu/tech/articles/970915/15priv.htm> (5 May 2004)
- Houston, E. (2004) "E-mail privacy at work, monster in human resources"
http://hr.monster.ie/articles/email_privacy/print (4 December 2004)
- Sinrod, E.J. (2003) "Electronic surveillance in the workplace"
<http://www.usatoday.com/life/cyber/ccarch/2001/10/18/sinrod.htm> (5 May 2003)
- Thompsons Solicitors (2006) "Employee surveillance"
<http://www.thompsons.law.co.uk/ltxt/11240005.html> (17 August 2006)
- Unknown (2003) "Dow Chemicals fires 50 over e-mail abuse"
<http://www.usatoday.com/life/cyber/tech/cti298.htm> (3 January 2003)
- Unknown (2004) "Welcome in ingenuity"
<http://www.ingenuity.co.uk> (5 December 2004)
- Withers, S. (2005) "Cyberbludging special: Acceptable usage"
<http://www.znet.com.au/news/business> (9 May 2005)

ABOUT THE AUTHOR

Verine Etsebeth is a lecturer in the Department of Private Law at the University of Johannesburg, South Africa.

Papers presented at conferences:

- 6th Annual Conference on World Wide Web Applications (1-3 September 2004 – Johannesburg) “*Corporate Responsibility for Information Security Governance*”
- 7th Annual Conference on World Wide Web Applications (1-3 September 2005 - Cape Town) “*Malware: The New Legal Risk to Companies*”
- Information Security South Africa ISSA 2006 “*Information Security Policies, Procedures, Standards and guidelines – The Legal Risk of Uninformed Personnel*”
- 8th Annual Conference on World Wide Web Applications (6-8 September Bloemfontein) “*Companies Beware: Inappropriate Use of Corporate Computer Resources and Systems*”

Publications in accredited law journals:

- TSAR 2005 2 “Governance in the Information Age – The Implication for Law”
- TSAR 2005 4 “Risky Business – risk management in the information age – is your business up for the challenge?”
- TSAR 2006 3 “The Growing Expansion of Vicarious Liability in the Information Age Part 1”
- TSAR 2006 4 “The Growing Expansion of Vicarious Liability in the Information Age Part 2”

Conference related publications:

- ISBN 0-620-35079-2 “Malware: The New Legal Risk to Companies” 2005
- ISBN 1-86854-636-5 “Information Security Policies, Procedures, Standards and guidelines – The Legal Risk of Uninformed Personnel” 2006
- ISBN (will still be assigned) “Companies Beware: Inappropriate Use of Corporate Computer Resources and Systems” 2006