WHY INFORMATION PRIVACY AND THE EMPLOYMENT RELATIONSHIP DON’T MIX: WORKPLACE E-MAIL AND INTERNET MONITORING IN THE UNITED KINGDOM AND CANADA

by

Hazel Dawn Oliver

A thesis submitted in conformity with the requirements for the degree of Master of Laws

Graduate Department of Law
University of Toronto

© Copyright by Hazel Dawn Oliver, 2001
The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author’s permission.

L’auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L’auteur conserve la propriété du droit d’auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.
ABSTRACT

Why information privacy and the employment relationship don't mix:
workplace e-mail and internet monitoring in the United Kingdom and Canada.

Hazel Dawn Oliver
Graduate Department of Law
University of Toronto

This thesis is a comparative study of the law relating to workplace e-mail and internet monitoring in the United Kingdom and Canada. The thesis begins by considering why information privacy is important and how it applies to the workplace. Chapters two and three analyse the law in the United Kingdom and Canada, which is shown to be incoherent and contradictory. Chapter four examines how concepts central to the definition of privacy are deliberately being applied to the employment relationship in such a way as to result in contracting-out of the right of privacy, so failing to treat information privacy as a constraint on freedom of contract. Proportionality is proposed as a preferable way of reconciling employee rights with employer interests. In the concluding chapter it is suggested that the reluctance to recognise information privacy rights in employment is due to the fact that privacy protection involves a direct interference with management prerogative.
ACKNOWLEDGEMENTS

First of all, many thanks to my supervisor Brian Langille for his support, encouragement, and constructive challenging of my work. I would like to give a special thanks to my second reader David Beatty, and also to Lisa Austin and John Craig for their invaluable comments and ideas relating to various parts of this thesis.

I would like to express my gratitude for the funding which I received for my studies, both to the Commonwealth Scholarship Commission for awarding me a Commonwealth Scholarship for study in Canada, and to the Faculty of Law at the University of Toronto for awarding me a Faculty Fellowship.

Finally, I would like to thank my colleagues on the L.L.M. and S.J.D. programs for the stimulating academic debate, culturally diverse experience, and of course the social life.
# TABLE OF CONTENTS

1 PRIVACY AND WORKPLACE MONITORING .............................................. 1

1.1 Introduction ............................................................................................................ 1

1.2 What is privacy and why is it important? ................................................................. 2
  1.2.1 What is privacy? ................................................................................................. 3
  1.2.2 The values served by privacy ............................................................................ 5
  1.2.3 The costs of privacy .......................................................................................... 8

1.3 Is the right of privacy applicable in the workplace? .................................................. 10

1.4 E-mail and internet surveillance in the workplace ..................................................... 16
  1.4.1 How can use of e-mail and the internet be monitored? ....................................... 17
  1.4.2 How e-mail and internet monitoring affects employee privacy ......................... 19

1.5 Employer justifications for e-mail and internet monitoring ...................................... 24

1.6 Privacy and employment .......................................................................................... 30

2 THE LAW IN THE UNITED KINGDOM ......................................................... 34

2.1 Workplace privacy in the UK before 2000 ............................................................... 34

2.2 The Human Rights Act 1998 .................................................................................. 37
  2.2.1 Application of the HRA to workplace privacy .................................................... 38
  2.2.2 Application of the HRA to e-mail and internet monitoring ............................... 42

2.3 The Regulation of Investigatory Powers Act 2000 .................................................. 48

2.4 The Data Protection Act 1998 ............................................................................... 60
  2.4.1 Application of the Data Protection Act to e-mail and internet monitoring .......... 60
  2.4.2 The Draft Code of Practice .............................................................................. 66

2.5 Conclusions ............................................................................................................ 70

3 THE LAW IN CANADA ....................................................................................... 72

3.1 Specific legislation relating to privacy .................................................................... 72
  3.1.1 The Criminal Code .......................................................................................... 73
  3.1.2 The Federal Privacy Act ................................................................................. 75
  3.1.3 The Personal Information Protection and Electronic Documents Act .............. 80
PRIVACY AND WORKPLACE MONITORING

"...monitoring and surveillance can be a source of fear and anxiety when used to exert excessive management control and to coerce workers to meet unrealistically high standards. Many workers feel pressure and intimidation from the feeling of being watched constantly. Stress researchers have identified intensive monitoring and control as stress factors in the workplace, which can lead to physical illness and psychological distress." (International Labour Office).

1.1 Introduction

Employers are increasingly adopting the practice of monitoring employee use of e-mail and the internet in the workplace. A recent American Management Association survey recorded that, "Nearly three-quarters of major US firms (73.5%) record and review employee communications and activities on the job, including their phone calls, e-mail, internet connections, and computer files." This problem is not limited to the United States, and there is increasing public concern in many jurisdictions about the ability employers have to snoop into their employees’ private lives. In today’s technological society, it is all too easy for employers to carry out pervasive surveillance of employee activity by electronic means, and such practices have potentially serious implications for employee privacy.

This issue raises questions about the specific problem of the legitimacy of employer surveillance of employees in the workplace, and also more general questions about how much privacy workers can be afforded within the context of an employer/employee relationship. Both the United Kingdom and Canada have begun the process of addressing these questions, and a comparative study of these jurisdictions is illustrative of various

---

1 International Labour Office Conditions of Work Digest, Volume 12 Part 1, Monitoring and Surveillance in the Workplace at 3.
3 See The Extent of Systematic Monitoring of Employee E-mail and Internet use (Privacy Foundation, Workplace Surveillance project, 2001) which found that 27% of the worldwide online workforce are under continuous online surveillance (as distinguished from more occasional spot-checks). (Report available at www.sonic.net/~undoc/extent.htm).
theoretical approaches towards electronic monitoring and workplace privacy. Overall, it appears that these approaches are weighted in favour of the employer’s interests at the expense of employee privacy. In comparing the United Kingdom and Canada, the aim is to consider why protection of workplace information privacy seems to be particularly problematic in the context of the employment relationship within a common law system. In particular, it appears that when concepts which are central to the definition of privacy itself are applied to the contract of employment, this results in the employer being able to control employee privacy expectations. It will be argued that this approach is inappropriate in light of the prevalence of external limitations on the parties’ freedom to contract in an employment relationship, and the importance of the right of privacy in today’s society.

This introductory chapter will consider the general questions of the definition of the right of privacy and the interests which it protects, the extent to which this is applicable in the workplace context, and then go on to discuss the specific issues of the ways in which e-mail and internet use can be monitored in the workplace and the reasons why this may be done. The following chapters will look at legal approaches to this issue in the United Kingdom and Canada. The fourth and concluding chapters will draw on UK and Canadian law in considering the more general theoretical issues of how information privacy is approached and defined, how it is applied within the employment relationship, and why the resulting protection of worker privacy is inadequate.

1.2 What is privacy and why is it important?

This section does not aim to provide an exhaustive definition of privacy and the values which it serves, a task which has already been attempted many times in various contexts and is beyond the scope of this thesis. There is a wide variety of often conflicting views on these topics. However, a brief review of some of the different definitions of privacy and the reasons why privacy can be seen as important will set the scene for subsequent discussions, and help to show why the issue of privacy in the workplace is the subject of so much debate at present.
1.2.1 What is privacy?

Privacy is notoriously difficult to define. The Younger Committee in the United Kingdom found the task so difficult that this was given as one of the reasons for recommending against the introduction of a general right of privacy in the UK. Various attempts have been made to describe the concept, all of which cover some of the central elements of privacy, but seem to fail to provide a satisfactory overall definition.

Perhaps the most well-known definition of privacy is that set out by Warren and Brandeis in their 1890 article in the Harvard Law Review, namely the "right of the individual to be let alone". This definition was put forward in the context of invasions into privacy by the press, and the article argued in favour of recognising privacy as an independent value. This somewhat wide and generalised definition has been built on subsequently by other authors.

For example, William Prosser has characterised the development of the American tort of invasion of privacy as made up of four separate torts: intrusion on an individual's seclusion or solitude, or into their private affairs; public disclosure of private facts; publicity placing an individual in a false light in the public eye; and appropriation of an individual's name or likeness. Other authors have attempted to produce a single definition. One common theme is that of control. Loss of control in any of these areas results in a loss of privacy. Arnold Simmel sees privacy as "the right to exclusive control of access to private realms". Others focus on the issue of privacy of information. Charles Fried describes privacy as control over "information" about ourselves. Alan Westin defines privacy as "the claim of individuals, groups or institutions to define for themselves when, how and to what extent information about them is communicated to others." A related approach is taken by Ruth Gavison, who

---

5 S. Warren & L. Brandeis, "The Right to Privacy" (1890) 4 Harv. L. Rev. 193 at 205.
7 A. Simmel, "Privacy" (1968) 12 International Encyclopaedia of the Social Sciences 480 at 482.
8 C. Fried, "Privacy" (1968) 77 Yale L. J. 475 at 482.
criticises use of "control" as the determining factor,\textsuperscript{10} relying instead on the test of whether we lose inaccessibility to others - the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention.\textsuperscript{11}

All of these attempts to describe privacy have something to commend them, but none seems to capture all of the circumstances in which privacy interests may arise. Indeed, it may be that a single understanding of privacy is simply not possible. On the basis that privacy is a creation of society, it can be said that the demand for privacy may differ significantly depending on the relevant society within which it is being considered, and therefore falls to be defined differently depending on social context.\textsuperscript{12}

One helpful approach towards understanding the various aspects of privacy is to break it down into different categories. This approach was taken by the Supreme Court of Canada in the case of \textit{R -v- Dyment},\textsuperscript{13} which concerned the legality of police use of a blood sample taken without consent. In his judgement, La Forest J describes three "zones" of privacy which may require protection - "those involving territorial or spatial aspects, those related to the person, and those that arise in the information context."\textsuperscript{14} Territorial privacy relates to protection of places and property. Personal privacy relates to the body and is violated by physical searches, including the taking of blood and other physical samples. Information privacy relates to the preservation of the confidentiality of information about individuals, and La Forest J emphasised the importance of this right in the modern world:

"In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but

\begin{flushright}
\textsuperscript{10} R. Gavison, "Privacy and the Limits of Law" (1980) 89 Yale L. J. 421 at 427-428. She argues that there are situations in which one may not have control over others' access to personal information but there is no loss of privacy until another person actually does access that information, and further that the notion of control suggests personal choice which may be to give up privacy as much as to preserve it.

\textsuperscript{11} \textit{Ibid.} at 423 and 428-429.

\textsuperscript{12} F. Cate, \textit{Privacy in the Information Age} (Washington D.C: Brookings Institution Press, 1997) at 22.

\textsuperscript{13} [1988] 2 S.C.R. 417.

\textsuperscript{14} \textit{Ibid.} at 428. This description of the three zones of privacy was taken by La Forest J from \textit{Privacy and Computers}, the report of the Task Force established by the Department of Communications/Department of Justice (Ottawa: Information Canada, 1972).
\end{flushright}
situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected.\(^{15}\)

It is primarily this last zone of information privacy which is most relevant to the issue of e-mail and internet monitoring, the subject of this thesis. Electronic surveillance of employees is potentially a threat to employee privacy largely because of the likelihood that the employer will obtain private information about employees – whether directly because this is the purpose of the monitoring, or indirectly as a result of surveillance for other purposes.\(^{16}\) If the focus is on information privacy, then perhaps Westin’s definition of privacy set out above (the ability of individuals to define how information about them is communicated), is the most appropriate one to bear in mind when considering the issue of e-mail and internet monitoring in the workplace. Although wide, this definition does appear to summarise the main concerns about such practices – namely, the fact that employees may thereby be denied the opportunity to define when, how and to what extent personal information about them is communicated to their employer.

1.2.2 The values served by privacy

A single definition of privacy may be difficult to achieve, but it is somewhat easier to identify the reasons why privacy is thought to be important. The most widely recognised values served by protection of privacy break down into two broad categories – those relating to autonomy and democracy, and those relating to dignity and personal wellbeing.

**Autonomy and democracy**

Personal autonomy relates to the ability of individuals to choose freely how to live their lives. It can be described as, “the desire to avoid being manipulated or dominated wholly by others”, and is vital to the development of individuality and individual life choices.\(^ {17}\) Autonomy is threatened by invasions of privacy, because individuals are deprived of the

\(^{15}\) Ibid. at 429-430.


\(^{17}\) Westin (1967) *supra* note 9 at 33.
opportunity to explore different options free from external observation and social pressures. Fear of penetration of an individual’s private “inner zone” will inhibit choices and the development of ideas, thoughts and feelings.¹⁸

Autonomy is thought of as particularly valuable in democratic societies. The development of independent thought and individuality is important in producing the diversity of views which allows for public debate and participation in political decisionmaking. Privacy allows individuals to develop their ideas before "going public",¹⁹ and can be described as essential to democratic government due to the way in which it fosters and encourages moral autonomy.²⁰ A society which protects privacy and so encourages autonomy and a diversity of life choices is also likely to be more pluralistic and tolerant than one in which individual choices are inhibited.²¹ As a related point, Westin emphasises that privacy also gives individuals space in which to process information, indulge in creative thoughts, and morally evaluate themselves.²² Again, this can be seen as assisting the process of democracy by encouraging citizens to think for themselves and develop ideas in an uninhibited way before making them public.

Autonomy can also be affected by invasions of privacy even where individuals do not know for sure whether or not this is occurring. Simply suspecting that one may be subject to surveillance can have a "chilling effect" on the exercise of other rights.²³ This is particularly the case with collection of personal data about individuals, where the knowledge that even participation in ordinary political activities might lead to surveillance can have a limiting effect on individual conduct.²⁴

In summary, as expressed by La Forest J in R – v- Dyment,²⁵ privacy is important because "the restraints imposed on government to pry into the lives of its citizens go to the essence of

---

¹⁸ Ibid. at 34.
¹⁹ Ibid.
²⁰ Gavison (1980) supra note 10 at 455.
²¹ Ibid.
²² Westin (1967) supra note 9 at 37.
a democratic state".  

Dignity and personal wellbeing

Another set of reasons why privacy is valuable deal with more personal issues of dignity and wellbeing.

A number of commentators see privacy as important to dignity. Warren and Brandeis, in the context of press intrusions into private lives, emphasise the "mental pain and distress" which is caused by such behaviour. 27 Edward Bloustein sees invasions of privacy as an affront to "personal dignity". 28 He emphasises that individuality includes the right to be free from certain types of intrusions, and this is of the very essence of personal freedom and dignity. 29 Intrusions into privacy are wrong because they amount to an "assault on the human personality" and are "demeaning of individuality". 30 Similarly, Simmel describes invasions of privacy as an offence against the rights of personality, namely individuality, dignity and freedom. 31

Protection of privacy can also be seen as important to emotional wellbeing. Private time and space gives individuals the opportunity for emotional release, which is important for both physical and psychological health. 32 As described by Westin, this need for release includes: the ability to be oneself in "off stage" moments; the opportunity for occasional minor non-compliance with social and institutional norms; the safety-valve function of being able to vent anger at authority figures or institutions in private; and the ability to deal psychologically with loss, shock or sorrow. 33

25 Supra note 13.  
26 Ibid. at 427-428.  
27 Warren & Brandeis (1890) supra note 5 at 196.  
29 Ibid. at 973.  
30 Ibid. at 974.  
31 Simmel (1968) supra note 7 at 485.  
32 Westin (1967) supra note 9 at 34.  
33 Ibid. at 35-36.
Privacy can also be viewed as providing scope for limited and protected personal communication, in particular the opportunity for sharing confidences and being intimate with trusted individuals, as well as allowing boundaries of mental distance to be set.\(^34\) Fried sees the development of intimate relationships as the most important function of privacy. Indeed, he states that fundamental relations such as respect, love, friendship and trust would be "inconceivable" without privacy, which is why a threat to privacy can be seen as a threat to "our very integrity as persons".\(^35\) Privacy allows individuals to be intimate with each other by voluntarily sharing private information, to trust each other with confidences, and to define their relations with each other as well as defining themselves.\(^36\) Without privacy, such fundamental intimate relationships simply could not exist.

The importance of privacy to personal dignity and wellbeing has been expressly referred to by the Canadian Supreme Court. In *R v. Dyment*, La Forest J recognised that, in addition to its importance in the democratic state, privacy is "essential to the well-being of the individual", and for this reason alone would be worthy of constitutional protection.\(^37\) In *R v. Mills*,\(^38\) the Supreme Court cited Fried's work with approval and noted that many commentators saw privacy as related to fundamental human relations, commenting that privacy is "essential to maintaining relationships of trust".\(^39\)

1.2.3 The costs of privacy

As can be seen from the above discussion, it is possible to identify a number of different values which are served by privacy. Some of these relate to personal freedom and personality, and others relate to the wider aims of the democratic state. Privacy is so important simply because it facilitates and protects these various crucial values. However, it

\(^{34}\) Ibid. at 38.
\(^{35}\) Fried (1968) *supra* note 8 at 477.
\(^{36}\) Ibid. at 479-486
\(^{37}\) *Supra* note 13 at 427.
\(^{39}\) Ibid. at 722-773. This case involved a constitutional challenge to certain parts of the *Criminal Code* which regulated production of personal records, arising from the issue of whether therapeutic records relating to the complainant in a criminal trial should be produced for the purposes of the accused's defence. The provisions of the *Criminal Code* were found to be constitutional.
must also be recognised that privacy has costs – it is not a “free lunch”.\(^{40}\)

The issue of setting appropriate limitations on the right of privacy was recognised by Warren and Brandeis, who state that determining in advance the exact line where “the dignity and convenience of the individual must yield to the demands of the public welfare or of private justice” would be a difficult task.\(^{41}\) The problem is that privacy can have some serious societal costs. Indeed, in some cases the exercise of privacy can go so far as to create dangers for democracy.\(^{42}\) As described by Westin, these dangers may include such issues as: indifference on the part of citizens to political and governmental needs due to private-life commitments; the growth of anonymous organisational influences over public life fostered by organisational privacy; unjustified privacy claims which prevent fair reply and fair criticism of those in public life; impediments to crime prevention and internal security caused by prevention of new law-enforcement methods; frustration of the public’s need to know; and the ability of governments to use privacy to cover up abuses of power.\(^{43}\) Protection of privacy in some circumstances may also pose particular dangers to public safety and public health.\(^{44}\)

The costs of privacy are particularly obvious in the case of information privacy, which can have clear societal costs because it does not depend on the content or merit of the information at issue.\(^{45}\) Posner has argued that much of the demand for privacy concerns either “discreditable information” or exploitation of other’s misapprehensions, and often the motive for concealment of information is in order to mislead others.\(^{46}\) It can be said that the protection of information privacy “facilitates the dissemination of false and misleading information, increases the cost of providing products and services, and interferes with

---


\(^{41}\) Warren & Brandeis (1890) supra note 5 at 214.

\(^{42}\) Westin (1967) supra note 9 at 25.

\(^{43}\) Ibid.

\(^{44}\) See in particular A. Etzioni, The Limits of Privacy (New York: Basic Books, 1999), who examines the tension between privacy and public health and safety in the specific contexts of the HIV testing of infants, the privacy of sex offenders, the deciphering of encrypted messages, the use of identity cards, and disclosure of medical records.

\(^{45}\) Cate (1997) supra note 12 at 23.

meaningful evaluation of students and employees". It is therefore in constant tension with other values.

If privacy is seen as a value of fundamental importance which is worthy of protection, then it must be recognised that its costs are often worth bearing. An appropriate balance certainly needs to be struck in any society between privacy and other values. However, privacy does serve many vital functions, and should not be given away too lightly. This issue of striking the appropriate balance between individual privacy interests and other interests is discussed further below in the specific context of the employment relationship.

1.3 Is the right of privacy applicable in the workplace?

The right of privacy appears to be established as a human right which protects important human interests. However, it can be argued that nevertheless it is not appropriate in a workplace setting. There are two main arguments in favour of this approach.

Firstly, the right to privacy can be seen as primarily designed to protect individuals against information-gathering and intrusion into the private sphere by the state. As discussed above, one of the major reasons why privacy is seen as so valuable is that it furthers autonomy and participation in political decision-making, and thereby the process of democracy. Government intrusions into privacy can be seen as particularly damaging, inhibiting the development of ideas and political activity in a way which is incompatible with a free society. The state is also in a particularly powerful position in relation to its citizens, with the resources to facilitate widespread use of privacy-invasive practices. It can therefore be argued that the right of privacy is much less important in the area of relationships between private parties, including the employment relationship.

However, this approach can be criticised in a number of ways. Although autonomy and the functioning of democracy can be inhibited by state intrusions into private life, intrusions by

\[47\] Cate (1997) supra note 12 at 102.
private individuals or organisations may also have the same effect. Development of free thought and behaviour can be inhibited if individuals fear being the subject of social criticism or ridicule, and this can be caused as much by private as by governmental invasions of privacy. In his famous essay “On Liberty” published in 1859, John Stuart Mill recognised that the “tyranny of the prevailing opinion and feeling” stemming from societal pressures could be more formidable than many types of political oppression.48

There are also a number of other values served by privacy which are not dependant on actions by the state. Issues of dignity, emotional wellbeing, and the ability to form relationships, are all equally affected by state or private action. Although the extent of the threat to individual liberty may be greater if privacy is invaded by the all-powerful state, it can be said that the “wrong” of the intrusion is the same in both cases.49 It should also be noted that a number of jurisdictions have specifically enacted legislation which protects the right of privacy as between private individuals and organisations.50 and a tort of invasion of privacy is recognised in the United States.

The distinction between state and private invasions of privacy breaks down further when one considers the specific issue of the employment relationship. It can be argued that the employer occupies a position of power in relation to its employees analogous to that of the state in relation to its citizens, and the workplace is a “microcosm of society at large”51. In his classic work on UK labour law, Kahn-Freund described the phenomenon of “social power” as being “the same no matter whether the power is exercised by a person clothed with a ‘public’ function, such as an officer of the Crown or of a local authority, or by a ‘private’ person, an employer, a trade union official, a landlord regulating the conduct of his tenants.”52. The nature of the employment relationship does inevitably require employees to give up some degree of individual autonomy in furtherance of the employer’s objectives, but

49 Bloustein (1964) supra note 28 at 975.
50 See for example the Privacy Acts enacted in British Columbia, Manitoba, Saskatchewan and Newfoundland (discussed in section 3.1.4 of chapter three), and the Data Protection Act 1998 in the United Kingdom (discussed in section 2.4.1 of chapter two).
it can be said that employees only consent to this limitation of autonomy to the extent that there is a sufficient link between those limitations and job performance. Employers have particular power to limit worker autonomy through invasions of privacy, which may need to be controlled – "To be an employee is to be enmeshed in a hierarchical structure of subordination that is quite at odds with any claim of individual autonomy even over arguably private spheres of endeavour."

It can in fact be said that preservation of worker autonomy is in the employer’s own interests. Independence of thought and creativity is important in the workplace as in society at large, and privacy-invasive practices may inhibit this in a way which is damaging to the employer’s business. Dignity and emotional wellbeing can clearly be affected by employer intrusions into privacy as by intrusions outside the workplace. There is also substantial evidence that privacy-invasive practices in the workplace, particularly pervasive surveillance, can cause actual psychological damage and stress-related illness. For example, the International Labour Office has specifically noted that the use of monitoring and surveillance as a management technique has serious consequences for working conditions and worker health. It can further be argued that protection of privacy is important in ensuring a healthy relationship between employer and employee, in which trust, respect and loyalty are important – employees who feel due to employer invasions of privacy that their dignity is not respected and they are not trusted are likely to lose loyalty and motivation, and productivity may consequently be affected. As expressed by Linowes and Spencer:

"Nothing can be considered right from the standpoint of efficiency if it is wrong morally. Those who think there is a basic conflict between long-term management effectiveness and safeguarding personal privacy rights must either be inexperienced in the art and science of management or ignorant of the consequences of personal privacy abuses. Full freedom is as

56 ILO (1993) supra note 1 at 11 (see the quotation at the start of this chapter).
57 Some jurisdictions imply notions of trust and good faith into the employment contract, such as in the United Kingdom where a mutual duty of trust and confidence between employer and employee is implied into all employment contracts (discussed in section 2.1 of chapter two infra note 119).
necessary to the health and vigour of business as it is to the health and vigour of citizenship.\footnote{59}

The second main argument in support of the idea that the right of privacy is inapplicable in the workplace is the view that when an individual is at work he or she is simply not on "private time". The employer has control over the workplace, including its contents, facilities and working methods, and therefore by entering the workplace the individual is giving up all expectations to privacy\footnote{60} - private life is for after working hours. This approach is particularly relevant to the issue of monitoring in the workplace. Arguably it is generally felt that "employees who enter an employer's premises to do paid work have left 'private' space and entered a 'public' arena", where they should expect to be observed by their supervisors.\footnote{61}

However, the argument that individuals can have no expectation of privacy at work is not really sustainable. As Westin points out in his earlier work, humans have a psychological need for privacy, which is essential to the effective operation of social structure.\footnote{62} In particular, total surveillance can only be survived by those with an absolute commitment to the "ideal of perfection" and this is "not the condition of men in ordinary society";\footnote{63} he goes so far as to describe total physical surveillance as "psychologically shattering"\footnote{64}. This need for privacy, and in particular the inability to tolerate constant surveillance, is equally as applicable to the society of the workplace as elsewhere. Although individuals are to a large extent under the control of their employers while at work, it is simply not possible for the basic human need for privacy to be given up entirely during working hours. To put it another way, it can be argued that the identity of workers as autonomous individuals is not shed as soon as they enter the workplace.\footnote{65} In relation to monitoring of employees, it is certainly true

\footnotesize
\begin{itemize}
\item \footnote{59}{D. Linowes & R. Spencer, "Privacy: the Workplace Issue of the 90s" (1990) 23 John Marshall L. Rev. 591 at 619.}
\item \footnote{60}{D. Banisar, Privacy & Human Rights: an International Survey of Privacy Laws and Developments (Washington D.C, Electronic Privacy Information Centre; London: Privacy International, 2000) at 47.}
\item \footnote{61}{A. Westin, "Privacy in the Workplace: how well does American Law reflect American Values?" (1996) 72 Chi-Kent L. Rev. 271 at 276.}
\item \footnote{62}{Westin (1967) supra note 9 at 58.}
\item \footnote{63}{Ibid. at 59.}
\item \footnote{64}{Ibid.}
\item \footnote{65}{B. Bilsen, "Search and Surveillance in the Workplace: the Employer's Perspective" in W. Kaplan, J. Sack & M. Gunderson ed Labour Arbitration Yearbook (Toronto: Butterworths, 1992) at 154.}
\end{itemize}
that a degree of supervision at work is to be expected. However, it seems obvious from a common sense standpoint that some types of monitoring are objectionable – surveillance carried out in workplace washrooms for example. It can also be said that all types of monitoring may potentially affect employee privacy, including electronic surveillance – “the uses to which the technology is put may be invasive, just as the uses of human supervision may be invasive.”66 Workplace electronic performance monitoring in particular can be a pervasive and constant presence which approaches “total surveillance”, effectively eliminating any privacy rights at all.67

The employment relationship can also be seen as more than something involving complete power and control by the employer. It can be argued that, rather than simply being sacrificed entirely to corporate objectives, workers invest much of their lives in their workplace and have an interest in the maintenance of working conditions which acknowledge their existence as autonomous beings.68 This seems to be even more the case in today’s society, where the traditional “nine-to-five” working hours are no longer the reality for many workers, and working hours often begin early and continue into the evenings and weekends. In these circumstances, it becomes even more “implausible” to expect employees to put their private lives on hold and devote 100% of working time to work related matters.69 This is particularly true of private communications – it seems inherently unreasonable to prevent all private communications by workers during the course of a long working day, especially as some workers may have no choice but to carry out some private business during working hours.70 If the line between working and private time is becoming increasingly blurred, surely it is unrealistic for employers to expect total control over an employee’s activities throughout an extended working day. To quote the previous Privacy Commissioner of Canada, “…employees have a legitimate interest in a reasonable quality of work life, and privacy is an essential element of that.”71 The present Privacy Commissioner of Canada takes a similar view, stating in a recent speech, “If privacy is a fundamental human right and a

66 Finkin (1996) supra note 54 at 265.
68 Bilsen (1992) supra note 65 at 144.
69 Morgan (1999) supra note 55 at 901.
71 Ibid. at 10.
social good, that right does not disappear when we pass through the door of the workplace. In fact, I cannot imagine a place where our rights need to be more respected than in the workplace, where we spend so much of our time and where so much of our life is defined.\textsuperscript{72} Of course, it can be said that the realities of the workplace require some compromise of values such as privacy and autonomy, in order that the employer can plan and control work effectively.\textsuperscript{73} However, the question is one of where this compromise and balance should be struck, rather than whether individuals can be denied privacy protection altogether when at work.

A related argument often used to deny workplace privacy focuses on the employer’s property rights – for example, the employer owns the workplace computer system, and therefore has a right to prevent abuse of its property. However, this confuses the question of whether there can be a privacy right in the workplace at all, with the question of which employer interests may be set against that right. Certainly this is a valid consideration in deciding whether an employee’s privacy rights will be afforded protection in a set of specific circumstances, and employer justifications for e-mail and internet monitoring are considered further in section 1.5 below, but it is not appropriate for such issues to have a bearing on the very existence of workplace privacy itself.

Employees can therefore expect some degree of privacy even while ostensibly at their employer’s disposal during working hours. To do otherwise would effectively deny the fact that employees bring themselves as individuals to the workplace, including the need for respect for their private lives. As will be seen from the discussions about UK and Canadian law in the following chapters, both of these jurisdictions accept that an individual can have some expectation of privacy in the workplace. It is the nature and degree of this right, rather than its existence, which is the contentious issue.

\textsuperscript{72} See the text of George Radwanski, Privacy Commissioner of Canada’s address to the University of Toronto and Lancaster House Conference on New Developments in Workplace Privacy, 6th April 2001 (available at www.privcom.gc.ca/speech).

\textsuperscript{73} Bilsen (1992) \textit{supra} note 65 at 154.
1.4 E-mail and internet surveillance in the workplace

Turning to the specific issue of e-mail and internet monitoring by employers, there is no doubt that this can have an enormous effect on privacy in the workplace. As referred to above in the discussion about definitions of privacy, this is a practice which primarily has an impact upon information privacy interests. Employers can gather information about employees by watching what they are doing during working hours, discovering their interests and private activities as revealed by e-mail and internet use, and even by simply reading their personal electronic correspondence. It is the technological revolution which has put these tools at the employer’s disposal.

The growth of the internet has clearly added to the ways in which an employer can obtain personal information about employees. The increased use of electronic monitoring and surveillance as a management technique, including e-mail and internet monitoring, has changed the methods used by employers to monitor productivity and work performance.74 These new methods of gathering information about workers can be seen as particularly problematic as compared to traditional forms of physical supervision because employers have the ability to carry out the monitoring secretly, and because monitoring can be continuous and all-encompassing.75 The technology makes prying into the private lives of employees both easier for the employer, and harder for the employee to detect.76

With specific reference to the internet, Frederick Schauer sees this development as both a quantitative and a qualitative change.77 Firstly, the internet has simply increased the quantity of information which can be accessed easily. Numerous databases can be reached and consulted from one computer terminal; this information might have been available before the advent of the internet, but it would have been much more difficult to access. In the context of the workplace, new technology has simply made monitoring of employee communications much easier. Employers previously had the ability to monitor employee letters and telephone

74 Ibid. at 111.
calls, but this was difficult and time consuming. The internet has not introduced a new type of information-gathering, but has increased the ease and frequency of access to such information, and thereby increased the dangers to employee privacy.\textsuperscript{78} Secondly, the ability of modern information technology to accomplish new things (rather than old things in an easier way), has introduced a more qualitative change, involving new ways of invading privacy.\textsuperscript{79} Schauer illustrates this point with a further workplace example, involving use of pornographic material in the office. An employee who wished to view sexually explicit magazines at work could easily keep this from the knowledge of his employer by locking the material away, but access of such material on the internet makes information about the employee’s activities immediately available to the employer.\textsuperscript{80} This change in quantity and quality can also be seen in relation to employee performance. Employers can check up on employee performance through electronic monitoring much more easily then through actual surveillance by supervisors (a change in quantity), but can also do so covertly without the employee’s knowledge, something which is not generally possible through physical supervision (a change in quality).

Overall, it can be said that the practice of e-mail and internet monitoring does pose new challenges to employee privacy. To a large extent this can be seen as a new example of an old problem – employers have always had the ability to obtain personal information about their employees in various ways, and the new technology has simply added to this ability (whether quantitatively or qualitatively) rather than introducing an entirely new concept.

1.4.1 How can use of e-mail and the internet be monitored?

It is worth considering briefly the range of powers which employers now have when utilising new internet technology, in order to understand fully the various ways in which employee privacy interests may be affected.

Modern networked systems provide the network controller with a great deal of power to

\textsuperscript{78} \textit{Ibid.} at 558.
\textsuperscript{79} \textit{Ibid.} at 559.
\textsuperscript{80} \textit{Ibid.}
obtain information about activity which is taking place on the system. For example, employers can look at individual computers to discover what software is being run and in what manner, and an audit trail can be produced which gives the employer a profile of each user and how they are interacting with their computer. Managers can monitor keystrokes, the amount of time which a computer is not being used during working time, and can remotely modify or suspend programs on any networked computer. Many systems also allow computer “peeking”, where a manager can log remotely into an individual’s computer in “real time” and watch the activity on that computer screen without the individual’s knowledge.

There are a number of ways in which e-mail and internet use can be monitored and observed. Most simplistically, many companies use “firewalls” which simply block potentially damaging incoming and outgoing communications. However, other employers go further. Quite apart from the ability to see remotely what an employee is doing on their computer screen at any one time, both e-mails and internet use can be specifically targeted. Employers can randomly review the content of e-mail messages, or utilise software which catches messages containing particular keywords or phrases which can then be reviewed. Employers may simply analyse “traffic data”, which gives information about the sender and recipient of e-mails, and possibly the title of the relevant message. However, it is very easy to go further and access the full content of the message. Even messages which have been “deleted” by an employee may remain stored on the network and can still be accessed by an employer. In relation to internet use, employers can obtain records of the sites visited by any individual on their computer, together with the overall time spent accessing these sites, and can also search the network’s files for any downloaded material.

The range of monitoring powers available to the modern employer can be illustrated by consideration of a couple of electronic products which are presently being advertised on the internet. “Esniff” is described as a product which can analyse all traffic data, including e-
mails, for either activity or content which has been defined as inappropriate by the network controller. The system then automatically produces a report on each network “abuse”, together with a copy of the offending material. In the case of an “inappropriate” workplace e-mail, this would be detected by the system and a copy of its content provided to the employer. Taking internet surveillance even further, “SilentRunner”\textsuperscript{85} has been developed by a company called Raytheon, which was previously a US defence contractor. This powerful product monitors both the flow and nature of traffic on a computer network, and allows the network controller to see everything which is happening on the system, from an overview to a profile of an individual employee. Employers can carry out real time auditing and monitoring of employee activity, including e-mail and internet use, in a way which is undetectable by the system’s users.

In light of new technology such as the two examples set out above, it is hardly surprising that e-mail and internet monitoring by employers is on the increase. In the 2000 American Management Association Survey on workplace testing, monitoring and surveillance, 38.1\% of respondent companies admitted to storage and review of employee e-mails, and 54.1\% admitted to monitoring of internet connections.\textsuperscript{86} It is clear that the practice is growing. However, does this actually have an impact on privacy? What are the various ways in which employee privacy may be affected by such surveillance?

1.4.2 How e-mail and internet monitoring affects employee privacy

Information privacy interests of employees can be infringed in a number of ways by e-mail and internet monitoring, some of which are less obvious than others.

Perhaps the most obvious example is that of deliberate monitoring of the content of personal e-mails, whether through real-time monitoring, or storage and later retrieval of the messages. An employer who reads the content of such communications is clearly obtaining personal information about its employees relating to their private lives. Similarly, an employer who

\textsuperscript{85} See www.silentrunner.com.
\textsuperscript{86} AMA (2000) supra note 2.
looks at non-business related internet sites visited by its employees will be obtaining personal information about them, including such matters as details of their interests and lifestyles outside work. Linking this back to the values identified in section 1.2.2, private communications by employees will be inhibited by such conduct – so having an impact on personal autonomy and the development of ideas, as well as personal dignity and wellbeing.

However, the effect of monitoring and surveillance practices on privacy is somewhat wider than these extreme cases. For example, an employer may choose to monitor "traffic data" rather than the actual content of communications. Although less personal information may be obtained through this method than through content monitoring, employee privacy may still be affected. An employer will obtain information about the people with whom the employee has communicated through their e-mail addresses, and the titles of e-mail messages may also reveal their subject matter and some or all of their content. Monitoring of the names of internet sites visited would similarly reveal information about an employee's private activities. Even firewalls could potentially reveal personal information about employees. For example, a networked system can be set up to block pornographic e-mails or internet sites. If an employee communication is stopped by the firewall, the employer would know that the employee had been attempting to access such information without needing to review the content, title or source of the communication. These examples may involve a less serious infringement of privacy than content monitoring, on the basis that less detailed information is being obtained, but nevertheless such practices can have an impact on employee privacy interests – dignity is still affected, and conduct may still be inhibited.

Employers may also affect employee privacy through e-mail and internet monitoring purely unintentionally, in circumstances where the monitoring in question is not designed to collect personal information at all. Some might not see this as an invasion of privacy. In the context of telephone monitoring, Westin has argued that it offends "reason and common sense" to claim a privacy right over business calls, as they involve the employer's equipment being used in the course of the employer's business. However, it must be recognised that private information can effectively be obtained as a "side effect" of monitoring for other purposes.

---

For example, e-mails and internet communications might be monitored for the purposes of quality control, in order to check that employees are communicating appropriately with clients and customers. As an inevitable part of this process, private communications will also be scrutinised by the employer, and it may be difficult or even impossible to separate private from business matters in advance. This problem of over-inclusiveness has already been recognised by employers in the context of video surveillance in the workplace - cameras directed at the production process will also catch every "twitch and scratch" of the workers, and it is not obvious how the irrelevant private information can be filtered out. A number of the business-related reasons for employer monitoring practices which are discussed further below, including virus prevention, protection of confidential information, and prevention of defamation and harassment, may result in the unintentional side-effect of monitoring of purely private communications. It would, of course, be possible for employers to avoid some of this problem by implementing a policy that any workplace communications clearly labelled "private" would not be intercepted or read. However, this might not go far enough. Even an ostensibly business communication might also contain personal information not intended for the employer's eyes -- for example, the employee might send an e-mail to a client or colleague revealing personal reasons for postponing a business meeting. It therefore appears that any monitoring practice can at least potentially result in the collection of personal information about an employee. Although unintentional, from the employee's point of view such conduct can implicate the values discussed in section 1.3.7 as much as deliberate information-gathering activities.

An employee's privacy interests can also be affected even if the employer does not actually carry out intrusive monitoring. In particular, the mere threat of surveillance may be enough to cause concern about privacy, in circumstances where the employees do not know whether they are actually being watched or not.

---


89 Ibid.
The power of the threat of monitoring can be illustrated by Jeremy Bentham’s concept of the “Panopticon”, an ultimate surveillance model prison. Bentham planned that the hypothetical Panopticon would be built as a circular structure, so that prisoners housed in cells around the edge of the circle could all be observed by a single guard from a central watchtower. However, the guard could not be seen by the prisoners. This would result in effective control of the prisoners whether or not the guard was actually present. By creating an illusion of constant surveillance, the mere fear of the prisoners that they might be being watched would be enough to control their activities. Bentham recognised that this principle could be applied to other institutions, and this idea was discussed further by Michel Foucault in relation to the assertion of power and social control in other types of institution, including factories. The concept can be used in any case where a task or particular form of behaviour has to be imposed on a multiplicity of individuals, such as a workforce. If the practice is applied to employees, a spying supervisor would be able to "judge them continuously, alter their behaviour, impose upon them the methods he thinks best". Foucault states that the Panopticon induces in the inmate "a state of conscious and permanent visibility that assures the automatic functioning of power", and, more generally, the fact that awareness of being observed makes the individual "the principle of his own subjection". This analogy of the Panopticon is used by Jeffrey Reiman in the context of the threat posed to privacy by electronic monitoring, with particular reference to Intelligent Vehicle Highway Systems in the United States, a centralised system which collects information about individual travellers. Reiman sees this as an example of the "informational panopticon" created by the technology of today’s society, whereby information about individuals is made visible from a single point. This creates a real threat to privacy by denying the individual a

---

90 This example is given by the UK Information Commissioner in the Draft Code of Practice – the use of personal data in employer-employee relationships (Information Commissioner, October 2000) at paragraph 6.3. (Discussed in more detail in section 2.4.2 of chapter two).
91 See J. Bentham, The Panopticon Writings in Miran Bozovic ed. (New York: Verso, 1995). The concept of the Panopticon was described by Bentham in a series of letters written in 1787.
93 Ibid. at 205.
94 Ibid. at 204.
95 Ibid. at 201.
96 Ibid. at 203.
space free from actual or potential surveillance – "the risks that are posed by the informational panopticon come not from being seen, but from the knowledge that one is visible."98 In order to protect individual privacy adequately, "we will need not only to prevent the misuse of information, but to prevent the fear that it is being misused."99 As Westin has emphasised, known observation exercises a restrictive influence over individuals which has an impact on privacy.100 It also appears that knowledge of the possibility of observation can have the same effect. The surveillance technology of Bentham's day, which was based on the architecture of a building, has been replaced in the modern world by the power of electronic surveillance technology.

This analysis can equally be applied to employer monitoring of e-mail and internet use. Employees may be generally aware of such practices, an employer may have a policy which warns of the possibility of such monitoring, or the employees may even have consented to the practices by agreeing to a particular provision in the employment contract. By all or any of these means the workforce may be made aware that covert monitoring might be carried out. In such circumstances, there is no need for the employer to actually carry out the monitoring in order to control employee activities – the mere knowledge that use of the e-mail and internet may be subject to surveillance will cause employees to limit the amount of personal information which is communicated in this way. The feeling of constantly being "watched" which is thereby caused in the employees will limit their freedom to carry out personal activities at work, and so limit the exercise of their private interests, irrespective of whether or not the employer is actually collecting personal information at any one time. Again, autonomy, development of ideas, and personal dignity and wellbeing will all be adversely affected.

It therefore appears that employers can infringe employee privacy through all types of e-mail and internet monitoring, irrespective of the purpose for which it is carried out, and even by simply threatening to implement such practices in the workplace. On the basis that privacy is

98 Ibid. at 43.
99 Ibid. at 44.
100 Westin (1967) supra note 9 at 58 (which is seemingly somewhat inconsistent with his later assertion that surveillance of business communications does not involve privacy rights, supra note 61).
important in the context of an employment relationship as elsewhere, and the values served by privacy are equally as applicable in the workplace as in the rest of society, this is potentially a very serious issue.

However, this does not necessarily mean that all such activities by employers should be prohibited. Protection of privacy has its own costs. It simply means that privacy interests are often if not always engaged by monitoring practices and therefore need to be recognised and given appropriate weight. Employers can have a wide range of legitimate reasons for monitoring e-mail and internet use, which also require recognition.

1.5 Employer justifications for e-mail and internet monitoring

"Welcome to the age of new technology, where corporate issues like poor productivity, sexual harassment, and even corporate espionage are now just a click away..." ¹⁰¹

This quote from the publicity material for a computer network monitoring device, in an attempt to sell the product in question, portrays use of e-mail and internet technology by employees as a potentially serious threat to the employer. In a sense, this is no exaggeration. It seems that this new technology, although integral to the running of any modern business, also provides employees with a seemingly unique opportunity to damage their employers’ interests. The issue of e-mail and internet monitoring is therefore particularly interesting when one is considering employee privacy rights in the workplace. This is a “hard case”, as employers have good reasons for wanting to monitor which will need to be taken into account in deciding whether or not employee privacy rights can be upheld.

It certainly must be recognised that privacy rights in this area have to be tempered by employer interests, which can be described as the employer’s prerogative to control what goes on in the workplace, supervise employee performance, and to protect and control property.¹⁰² The main reasons put forward by employers in justification of e-mail and

¹⁰¹ Publicity quote from the website of esniff.com, supra note 84.
internet monitoring practices can be summarised as follows.

**Abuse of time and property**
Employers may want to monitor e-mail and internet activity in order to check that employees are not abusing the technology, in particular by sending excessive numbers of personal e-mails or surfing the net for personal purposes during working time. The amount of time wasted by employees using e-mail and the internet for private purposes is certainly a real problem for employers. The American Management Association survey for 2000\(^{103}\) reports that 44.8% of employers had disciplined employees for misuse or personal use of e-mail in the previous year, and 41.9% had disciplined for misuse or personal use of the internet. This is the paradigmatic example of circumstances where an employer can justify monitoring of personal communications. The employer must be able to distinguish between private and business communications in order to show that inappropriate use has been occurring, and therefore some screening of personal information is required.

**Loss of confidential information**
Confidential information and trade secrets can easily be disseminated by employees by e-mail and over the internet. This fear is traded on by companies selling monitoring technology, who emphasis the “insider threat” to the employer’s business.\(^{104}\) Monitoring can therefore be justified by employers on the basis that this is the best way to prevent leaks of such information.

**Prevention of competition**
Workplace e-mail and the internet may be used by employees for activities which are in competition with the employer’s business – whether preparing for a move to a competitor, or even running a competitive business using the employer’s technology during working time. Again, monitoring can be justified as the best way to prevent such activities.


\(^{104}\) See, for example, the claims of Raytheon that 70% of the loss of proprietary information is due to current and unauthorised employees and contractors, and use of the company’s technology is the only way to address that “insider threat”, *supra* note 85. See also Privacy Foundation (2001), which points out that employers are increasingly realising that most business security threats come from knowledgeable insiders rather than random outsiders.
Quality control
An employer may wish to monitor employee communications for the purposes of quality control – to check that employees are carrying out their tasks correctly, or to verify the quality of advice and assistance which is being provided to customers or clients. It is very common for monitoring of employee telephone conversations to be justified on this basis, and a similar approach can be taken towards e-mail and internet communications. This is a good example of circumstances where infringement of privacy may be an unintentional “side effect” of the monitoring. The justification of quality control only applies to business communications, but as discussed above it is extremely difficult to separate business from private communications in advance.

Liability for defamation
Defamation liability can arise as a result of e-mail or internet communications as much as through oral or other types of written communications. However, defamatory comments made by an employee using an employer’s computer system can cause particular problems. For example, in the United Kingdom it has been established that the employer can be held to have “published” the employee’s comments over its computer system and therefore be directly liable for defamation, even though the employee’s activities may have been entirely unauthorised by and unknown to the employer. In 1997 the Norwich Union building society had to pay some £450,000 to its client, the Western Provident Association, when a defamatory e-mail about the client sent from one employee to another came to that client’s attention.\(^{105}\) Prevention of such liability is therefore a further justification for e-mail and internet monitoring.

Prevention of harassment
E-mail and the internet provides employees with additional tools to carry out acts of workplace sexual or racial harassment, and other types of abusive behaviour towards co-

\(^{105}\) The e-mails in question concerned rumours spread by staff within Norwich Union’s health insurance arm that Western Provident was being investigated by the Department of Trade and Industry, and was in financial difficulties. See “NU to make e-mail libel payout”, the Times (London) 18 July 1997; “Norwich Union libel case alerts companies to dangers of e-mail”, The Lawyer 29 July 1997.
workers. Abusive or harassing messages, jokes and images can be sent easily and anonymously by using this technology. Employers can therefore justify monitoring on the basis of preventing such behaviour in the first place, and also as part of an investigation designed to catch the perpetrator of known harassment.

Prevention of pornography
Pornographic material can easily be obtained by e-mail or over the internet, whether written material or obscene images, and saved on an employer’s network. As well as the risk that this will cause harassment and distress to co-workers, employers may fear being criminally liable for illegal pornographic material which is stored on their computer system. As with prevention of harassment, monitoring may be justified in order to prevent such conduct, and in order to catch offenders.

Protection from computer viruses
Computer viruses can be contained in material downloaded from the internet, and in attachments to e-mails. They are often contained in seemingly innocent personal messages. The damage to an employer’s business which can be caused by the introduction of a virus into a computer network is illustrated by the spread of the “I love you” virus. Sent as an attachment to an e-mail, this virus devastated computer systems worldwide within a matter of hours. In order to protect their network from attack, employers may use a firewall to block and then screen suspicious messages and attachments, including in particular personal messages and jokes which may be used to disguise a potentially damaging virus.

Avoidance of bad publicity
Finally, e-mail and the internet is simply a very effective tool by which potentially damaging information about an employer can be disseminated by an employee extremely quickly. This may stop short of defamation or disclosure of confidential information, but even a seemingly

---

106 The virus was attached to an e-mail entitled “I love you”. When opened, this e-mail was automatically forwarded to everyone in the recipient’s address book, attacked other files on the computer system, and searched for confidential passwords. Simply due to the consequent volume of e-mail traffic, business computer networks were paralysed worldwide. See “Love bug bites all over the world”, the Times (London) 5 May 2000; “From hackers with love: the computer bug that brought world business to its knees”, the Independent (London) 5 May 2000.
innocent comment which shows the employer in a bad light can cause real damage if spread widely enough. Monitoring could simply be justified on the basis of preventing employees from making such potentially damaging communications. A somewhat frivolous example of this phenomenon is the spread of a very personal message about an individual called Claire Swires throughout the UK. Within hours this single e-mail had been forwarded throughout firms in the City of London, companies and workplaces in the rest of the UK, and to computer terminals worldwide.\textsuperscript{107} This illustrates just how quickly a potentially damaging e-mail can be spread.

As demonstrated by the above summary of the major reasons why employers may want to monitor e-mail and internet use in the workplace, the practice can be seen as integral to countering a variety of serious threats to the employer's business which can be caused by inappropriate use of technology. A parallel can be drawn here with Schauer's analysis of the growth of electronic surveillance as involving both a quantitative and a qualitative change.\textsuperscript{108} Some of these threats are a "qualitative" change as they are unique to e-mail and internet use, such as the spread of computer viruses or the liability of employers for defamatory comments "published" on their computer system.\textsuperscript{109} However, others appear to be a more "quantitative" change, involving new examples of old problems. Dissemination of confidential information, working in competition with an employer during the employer's time, and workplace harassment, are all types of behaviour which can take place without use of this new technology. Introduction of e-mail and the internet has simply added to the circumstances in which this behaviour can occur. It is therefore somewhat questionable whether e-mail and the internet is really such a new danger in all cases, and therefore whether pervasive monitoring practices are always justifiable or necessary if these infringe

\textsuperscript{107} See "Raunchy e-mails: it's time we all grew up", The Evening Standard (London), 15 December 2000 and "Yum yum: The saucy e-mail that wrecked Claire's life", The Sunday Times (London), 17 December 2000. The intimate e-mail was originally sent by Ms Swires to her boyfriend, who took the unwise step of forwarding a copy to six of his friends, following which the communication was rapidly forwarded throughout the country in a chain reaction.

\textsuperscript{108} Schauer (1998) supra note 77.

\textsuperscript{109} In relation to defamation, it can also be argued that there is a tendency to treat e-mail as an informal means of communication equivalent to verbal gossip, even though it results in a written record. This differs from the distinction generally drawn between gossip and written communications – see Post, "The Legal Regulation of Gossip: Backyard Chatter and the Mass Media" in R. Goodman and A. Ben-Ze'ev ed. Good Gossip (Lawrence, Kansas: University Press of Kansas, 1994) at 67 in relation to the legal regulation of gossip and the traditional difference in legal treatment between slander and libel.
employee privacy. As the Privacy Commissioner of Canada has recognised, "...vigilance should not be confused with hysteria. The surveillance systems [employers] introduce may have consequences far worse than the perceived problem they are set up to address."\(^{110}\)

Of course, workplace privacy has costs for the employer, just as privacy in general can have costs for society. These costs are the limitations placed on employers in pursuing the many aims set out above which are assisted by workplace monitoring. However, as already discussed, privacy protects a number of values which are held to be very important by society, and this is as true of the workplace as elsewhere. If privacy is worth protecting, then its costs will often be worth bearing. The key question is really one of where the balance should be struck between privacy rights and the employer's interests. It appears that all types of e-mail and internet monitoring practices can infringe privacy to some extent. However, it is a question of degree – if one monitoring practice is less privacy-invasive than another, at the very least it can be argued that the less invasive practice should be preferred.

It should also be noted that circumstances in which employers do have business reasons for electronic monitoring of employees are potentially the most dangerous towards privacy interests, because these justifications can be used to support pervasive monitoring practices and there is a temptation that they will not be questioned. As Matthew Finkin has argued, "The need for a law protective of privacy is summoned not only for the occasional outrageous intrusion by a manager off on a frolic, but far more where an employer acts in a systematically invasive fashion in what it takes to be a legitimate business interest."\(^{111}\) It is perhaps too easy for employers in today's technological society to rely on surveillance and monitoring of their workers without considering whether this is truly necessary:

"Today's workers face two daunting opponents: information-hungry employers who seem to have lost confidence in their ability to make hiring decisions and supervise without the aid of intrusive technology, and the surveillance technology companies that profit by persuading employers to pry into the lives of workers who are not in a position to resist."\(^{112}\)


\(^{111}\) Finkin (1996) \textit{supra} note 54 at 228.

\(^{112}\) Oscapella (1998) \textit{supra} note 51 at 342.
“Do you really believe that employees will cheat you and harass each other unless you treat them like unruly prisoners? Do you really need to treat all of your employees as suspects, just to catch some and dissuade the rest? Yes, you can monitor people, but should you?”

Certainly e-mail and internet monitoring can be a helpful management tool, and use of this technology by employees poses some real dangers for employers. It can also be said that the range of justifications which employers may have for privacy-invasive practices is particularly wide, encompassing general supervision, discipline, and protection of property and the employer’s business. These reasons are both more numerous and more compelling than the reasons which might be put forward to justify invasion of other rights, such as equality or freedom of expression, so making protection of information privacy in the workplace a particular challenge to an employer’s interests. However, it is important that employer justifications are given genuine scrutiny, in order to ensure that employee privacy interests are accorded appropriate protection. As will be seen in the following chapters on UK and Canadian law, in practice this is not always the case. Instead, there is a tendency to deny employee privacy rights altogether by deferring to the employer’s interests and management prerogative in supervising and running the workplace.

1.6 Privacy and employment

This chapter has established a number of aspects of the right to privacy. It is a very important right in today’s society which serves fundamental values. It can be applied in the workplace, and it is both appropriate and necessary to respect privacy within an employment relationship. E-mail and internet monitoring provide a clear example of the scope which employers have for invading employee privacy, and although protection of information privacy in this area may come into conflict with various employer interests it is nevertheless deserving of recognition. However, there remains the question of how privacy can be protected effectively within the context of an employment relationship. This issue will be discussed in detail in the final two chapters of this thesis, but it will be helpful to set the scene briefly at this stage.

113 George Radwanski, Privacy Commissioner of Canada, supra note 72.
The starting point is the basic approach towards the employment relationship taken in the common law jurisdictions of the UK and Canada. In both countries, the traditional approach is to treat the relationship as one of freedom of contract between the parties. The employer and employee are free to set the terms and conditions of employment with minimal external legal regulation – leaving individual rights, including privacy, as a matter of contractual negotiation between the parties. As will be discussed in the final chapter, there are a number of arguments as to why this purely contractual approach towards employment rights is not appropriate in today’s society.

With specific reference to privacy, this can be regarded as a human right potentially requiring protection in all circumstances, and therefore should be treated as a value which operates outside the employment contract. This means that the existence of a right to privacy in a particular workplace should not depend on the content of the employment contract. Privacy is such a fundamental value that the parties to the employment relationship should not be able to “contract out” of the right. As will be seen from the subsequent discussions of UK and Canadian law, both jurisdictions do to some extent treat the right to privacy in this way.

However, it also appears that there is a tendency in UK and Canadian law to allow the employer to effectively exert control over employee privacy rights, dictating when they will and will not apply. This is particularly the case with information privacy, as is illustrated by the example of e-mail and internet monitoring. As will be considered in detail in the chapter four, the problem is not necessarily with the definition of privacy per se, but rather the way in which concepts central to the legal definition of privacy interact with approaches towards the employment relationship. Although in theory protection of workplace privacy is not dependant on the content of the employment contract, in practice there is scope for “contracting out” of the right, which often renders the right to privacy entirely meaningless. This can be explained briefly as follows.

---

This is analogous to the treatment of other human rights, such as freedom of expression and the right not to be discriminated against, which can not be removed even by express contractual wording.
Firstly, the concept of "reasonable expectations" of privacy is used in both the UK and Canada in various contexts. It is somewhat unclear as to whether this is to be treated as a normative or an empirical concept. Both jurisdictions tend to treat the question of whether an individual has a reasonable expectation of privacy as an empirical one, meaning that the existence of a privacy right appears to depend on what an individual has been led to expect in the circumstances. This is particularly problematic in the context of an employment relationship, as most employers have the power to dictate conditions of employment and so control privacy expectations in the workplace. Although privacy is still operating as a value which exists independently of the contract, an individual's expectations about privacy can be set by the employer.

Secondly, both the UK and Canada treat the notion of "consent" as important to the concept of privacy. Aspects of the law in both jurisdictions take the approach that if individuals have consented to a potential invasion of privacy, this is not an infringement of the right. Again, in the context of an employment relationship, this can be problematic. The question is whether consent to privacy-invasive practices can really be meaningful within an employer-employee relationship, due to the inherent imbalance of power between the parties. The employer appears to have scope to obtain "consent" to infringements of privacy, whether explicitly through the employment contract or even implicitly through acquiescence to specific policies, in circumstances where in reality employees have no real choice but to agree.

When these issues are explored in much more depth in the final chapter, it will be seen that the problem is more than simply one of a bad fit between privacy concepts and the dynamics of the employment relationship. Although constrained to some extent by the doctrines of reasonable expectations of privacy and consent, in many cases the courts and legislators are actually using these concepts to defeat workplace information privacy rights, giving them a limited interpretation in the employment context. This attitude is somewhat surprising, as it contrasts with the treatment of other human rights and employment standards, which are more generally accepted as being legitimate limitations on freedom of contract. The rationale behind this approach is not clearly articulated. However, when faced with new
concepts such as the challenges to information privacy posed by computer technology, it appears that the law relies on traditional approaches towards the employment relationship which uphold the employer's prerogative to control the workplace. This can be seen as connected with the particular challenge which recognition of information privacy poses to management prerogative. Protection of information privacy in employment, particularly in relation to e-mail and internet monitoring, amounts to direct interference with the employer's ability to supervise and control the workplace - in circumstances where the employer has a particularly wide range of reasons for wanting to carry out privacy-invasive practices. This often results in deference towards the employer's interests, and outright denial of workplace privacy rights. Information privacy is therefore not being given the protection which befits its status as a fundamental human right, something which is particularly concerning in light of the vulnerability of many employees and the importance of privacy within the modern workplace.

The next two chapters of this thesis deal with the detail of UK and Canadian workplace privacy law, with specific reference to e-mail and internet monitoring. It will be seen that both jurisdictions protect privacy in various ways. Some of these provisions are not specifically related to the employment relationship but are general principles applied in a variety of contexts, while others directly consider the question of privacy in the workplace. Protection of privacy is very new to UK law, while in Canada the right has been established for some time. However, both jurisdictions rely on a patchwork of legislation and caselaw, and fail to take one coherent approach towards the issue. The final two chapters will draw together the themes which have emerged from the study of UK and Canadian law in providing an answer to the question as to why the application of information privacy rights within an employment relationship is often so unsatisfactory.
2 THE LAW IN THE UNITED KINGDOM

"...it should be no matter for surprise that the case for governmental intervention, based on fresh legislation, has seemed to us strongest in those fields where an entirely new threat to privacy seems to be imminent or has already arisen. This applies especially to the introduction of new technical, electronic and visual devices, their use by a wide range of people and organisations for various purposes gives a new and menacing dimension to familiar threats to privacy." (Younger Committee).115

No general right to privacy has traditionally existed in United Kingdom law. Employers have therefore been able to implement policies and practices which potentially infringe employee privacy in the workplace largely without fear of legal action. This situation has changed radically as a result of the three new pieces of legislation which came into force in 2000 – the Human Rights Act 1998 ("the HRA"),116 the Data Protection Act 1998 ("the DPA"),117 and the Regulation of Investigatory Powers Act 2000 ("RIPA").118 These do not introduce a general and universal right to privacy. However, each one of the statutes has an impact on workplace privacy generally and electronic monitoring in particular. The legislation is discussed in detail below. It will be seen that the law at present remains unclear, with the different pieces of legislation taking contradictory approaches towards the relevant issues. However, before turning to the existing state of the law, it is worth considering briefly the background to the current legal position.

2.1 Workplace privacy in the UK before 2000

Prior to the introduction of this new legislation, there was little if any limitation placed on the ability of employers to carry out electronic monitoring of their employees. Monitoring could be carried out so long as it was not in breach of the contract of employment at common law. Breach of contract could be avoided if the right to monitor was included as part of the employment contract itself, no matter how intrusive the practice in question.

115 Supra note 4 at 8.
116 The Human Rights Act 1998 c42.
117 The Data Protection Act 1998 c29.
If the contract of employment is silent on the issue of electronic monitoring, it is possible that particularly serious invasions of privacy by this means would amount to breach of the duty of trust and confidence which is implied into all contracts of employment. This might entitle the employee to resign and make a claim for wrongful dismissal and possibly also unfair dismissal. However, although this avenue of redress was (and still is) theoretically available to employees, perhaps somewhat surprisingly there is no existing line of caselaw which recognises breach of employee privacy as a breach of contract. This could be due at least in part to the fact that the potential for claiming breach of contract is somewhat limited. If employees knew of privacy-intrusive practices in the workplace but did not resign immediately in response, the employer could argue that they had impliedly "consented" to these practices by remaining in the workplace. An employer could further argue that any constructive dismissal was also in fact fair, on the basis that monitoring was carried out in furtherance of a legitimate business interest. In any event, the UK courts and tribunals have not in fact developed these arguments. This meant that, prior to the introduction of the new legislation, employees had no realistic remedy for intrusive workplace monitoring by employers.

The question of whether to introduce a general right of privacy into UK law has been

---

119 This implied duty was developed at first instance and applied by the Court of Appeal during the 1980s (see Woods v. WM Car Services (Peterborough) Limited, [1981] I.R.L.R. 347 and Lewis v. Motorworld Garages Limited, [1985] I.R.L.R. 465). The concept was recently confirmed by the House of Lords to be a requirement that the employer would not, without reasonable and proper cause, conduct itself in a manner calculated and likely to destroy or seriously damage the relationship of confidence and trust between employer and employee (Malik v. BCCI, [1997] I.R.L.R. 462).

120 An action for breach of the employment contract, based on the employee’s contractual notice period. Damages are based on the amount the employee would have earned during his or her notice period.

121 A statutory right, which can be relied on by all dismissed employees if the relevant preconditions are satisfied (including the need for one year’s continuous service). An unfairly dismissed employee can claim compensation of up to £50,000 for consequential lost earnings under section 112 of the Employment Rights Act 1996.

122 M. Ford, Surveillance and Privacy at Work (London: Institute of Employment Rights, 1998) at 30 and 32. Although it should be noted that the Employment Appeal Tribunal has emphasised that acquiescence in a breach of contract will only amount to an agreed variation in certain circumstances, and it must be considered whether the breach has had an immediate practical effect on the employee - if not, continuing to work after the change has been implemented is not necessarily enough to constitute consent to the change (see Jones v. Associated Tunnelling Co Limited, [1981] I.R.L.R. 477).

123 Ibid.
considered on a number of occasions. As far back as 1972, the Younger Committee produced a report on privacy which specifically considered the issue of workplace privacy and monitoring.\textsuperscript{124} The Committee had asked for public submissions on privacy issues, and received only ten letters about invasions of privacy by employers and potential employers.\textsuperscript{125} The Committee did not recommend that any new legislation be introduced in this area, stating that the issue could be dealt with as a matter of "good relations between employer and employee".\textsuperscript{126}

However, the Younger Committee did express some concerns about the growth of privacy invasive practices in the workplace, particularly in light of new technology. At this date, e-mail and the internet were unknown. However, there was recognition of the potential for new technology to create an increasing threat to privacy, and the Committee commented that the strongest case for new legislation was in this area: "This applies especially to the introduction of new technical, electronic and visual devices, their use by a wide range of people and organisations for various purposes gives a new and menacing dimension to familiar threats to privacy."\textsuperscript{127} As part of the report, the Committee carried out a survey by interview where specific questions were asked of members of the public. In the context of the workplace, participants in the survey were asked how they felt about a factory where closed circuit television cameras had been set up without explanation, which watched the main entrance, accounts office, main workshop, and entrance to the canteen. Some 62% of participants saw this as an invasion of privacy, and 61% stated that they would either be "a bit" or "very" annoyed or upset by such treatment.\textsuperscript{128} This seems to provide some evidence of genuine public concern about the use of technology to monitor employees in the workplace. Although the Committee itself did not recommend actual legislation to control overt workplace surveillance, this appeared to be largely based on the assumption that such matters would be the subject of consultation between management and workers, requiring management to justify the measures in question. "Good sense" between employers and employees would allow for reasonable overt use of surveillance for such matters as

\textsuperscript{124} Committee on Privacy (1972) supra note 4.
\textsuperscript{125} ibid. at 93 (although only 214 letters were received in total about all privacy issues).
\textsuperscript{126} ibid. at 95.
\textsuperscript{127} ibid. at 8.
prevention of pilfering and the control of processes, with the consent of employees' representatives.\textsuperscript{129} This seems to show a genuine concern that such practices should only be used where necessary and justifiable, and at the time collective consultation may well have seemed the best way to control the situation.\textsuperscript{130} Certainly the Committee was extremely opposed to secret monitoring: "...surreptitious surveillance in places of work would, in our view, be quite indefensible, because the employees, being ignorant of it, could take no measures to avoid it, and because justifiable supervision should not need to be surreptitious to be effective."\textsuperscript{131} However, negotiation and agreement with employee representatives is also seen as necessary even where the surveillance is known about by the employees.

Although the report of the Younger Committee did not result in any new legislation, it does show a fair degree of understanding and concern about the potential for new technologies to threaten privacy in the workplace. However, subsequent reports on whether to introduce a right of privacy into the law have tended to focus on other issues, without any specific consideration of the workplace.\textsuperscript{132} Therefore the issue of privacy at work, and the more specific issue of electronic monitoring by employers, has received very little attention since the report of the Younger Committee in 1972. It is seemingly only since the introduction of the new legislation discussed below that this topic has become a matter of real public concern and debate.

\textbf{2.2 The Human Rights Act 1998}

The HRA came into force on 2 October 2000, and implements most of the provisions of the \textit{European Convention on Human Rights} ("the Convention") into UK law. This includes Article 8, which reads as follows:

\begin{enumerate}
\item \textsuperscript{128} \textit{Ibid.} at 93.
\item \textsuperscript{129} \textit{Ibid.} at 171.
\item \textsuperscript{130} The Committee could not have predicted the future developments in UK collective labour law which severely undermined the importance of collective consultation and the power of the unions.
\item \textsuperscript{131} \textit{Supra} note 4 at 172.
\item \textsuperscript{132} The only other major report on privacy, the Calcutt Report (\textit{Report of the Committee on Privacy and Related Matters}, Chairman: David Calcutt QC (London: Home Office, June 1990)), was prompted by public concern about intrusions into private lives by the press, and focussed exclusively on protections from and remedies against press intrusions.
\end{enumerate}
"1. Everyone has a right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

This introduces a new right to privacy into UK law. However, the precise way in which the HRA will work in practice is somewhat complex, and some potential limitations on the applicability of the right should be noted.

2.2.1 Application of the HRA to workplace privacy

There are two potential limitations on the applicability of the HRA to workplace privacy issues. Firstly, the right to privacy is not unqualified. An interference with privacy under Article 8(1) can be justified under Article 8(2) if the relevant criteria are met. Any such interference must be "in accordance with the law", which means that provisions of other laws must not be breached (such as the DPA or RIPA, discussed further below). It must also be "necessary in a democratic society". This has been interpreted by the European Court of Human Rights ("the ECHR") as a proportionality test, involving a balancing of the seriousness of the infringement of the right in question against the importance of the interest being asserted against the right. The interests being balanced against the right must come within one of the categories listed in Article 8(2). However, potentially these are relatively wide. In particular, the concept of "the protection of the rights and freedoms of others" is not limited to other rights under the Act. In the specific context of infringements of privacy in the workplace, an employer could at least potentially assert a wide range of justifications for privacy-invasive practices which ostensibly protect its own or others' rights. A variety of such justifications are commonly put forward by employers in relation to the practice of email and internet monitoring, as discussed in some detail in section 1.5 of chapter one.

Secondly, the right is limited to interferences by a "public authority". Section 6(1) of the
HRA makes it unlawful for a "public authority" to act in a way which is incompatible with a *Convention* right. This means that the various rights under the HRA can only be asserted directly against public authorities, and therefore it is only employees of public authorities who can bring a direct claim for breach of privacy under the HRA. The concept of "public authority" includes "any person certain of whose functions are functions of a public nature", which appears to widen the category of employees who can bring claims to include those working for private bodies carrying out public functions, such as the privatized utilities. However, such hybrid bodies are not treated as a public authority if the nature of the act in question is "private". Although the question has not yet been tested in court, it appears likely that such bodies will be treated as carrying out private acts when acting as employers in dealing with their employees, and therefore the provisions of the HRA will not be directly applicable.

This seems to leave employees of public authorities as the only individuals who are able to assert a right of privacy under the HRA in the workplace. However, although the rights created by the HRA may not be directly enforceable by the majority of employees in the UK, they will nevertheless be very relevant to the development of employment law generally and workplace privacy rights in particular. Indeed, it is through this somewhat more indirect route that the HRA is likely to have its greatest impact on the law. The position can be summarised as follows.

The HRA is structured so that UK courts and tribunals must interpret both statute and common law in such a way as to uphold *Convention* rights. Firstly, courts are placed under an express obligation to read and give effect to primary and subordinate legislation in a way which is compatible with *Convention* rights whenever possible. Therefore cases utilising this new principle of statutory interpretation may affect rights and obligations between individuals, on the basis that such legislation may govern the relationship between...
private individuals as much as between individuals and the state. Secondly, courts and tribunals are expressly included within the definition of "public authority", and therefore bound to act in accordance with Convention rights. This includes circumstances in which courts and tribunals are developing and interpreting the common law, even where the law is being applied to decide private disputes between private parties. The courts therefore appear to be under an obligation to apply both statutes and the common law in a way which is consistent with fundamental human rights, including the right of privacy, irrespective of whether the claim in question involves a public or private body. This in turn opens up the possibility that a more generally applicable right of privacy will be developed by the courts.

In the specific context of workplace privacy, various provisions of UK employment law can potentially be interpreted so as to protect employees’ rights. In relation to the common law, as discussed above, privacy invasive practices could be seen as a breach of the implied duty of trust and confidence between employer and employee. Although to date this argument has not been developed by the courts, the influence of the HRA is likely to change the position, effectively implying workplace privacy rights into the contract of employment. In light of the fact that courts and tribunals are expressly bound to act in a way which is compatible with rights under the HRA, they appear to have little choice but to find that an unjustifiable invasion of privacy by an employer amounts to a breach of trust and confidence. This has been the experience of some other jurisdictions where there is a similar implied duty in the

---

138 Section 6(3)(a).
140 See The Lord Chief Justice, Lord Bingham, stated before incorporation that “…there will be no need for legislation. The courts have to be seen as an arm of the state for this purpose…there will be a clear duty on the courts to protect privacy and my experience is that, over time, they will develop the law.” (The Times (London) 9 October 1997). The prevailing view among legal commentators is that this will not result in the creation of new causes of action, but have indirect “diagonal” horizontal effect by impacting on the existing law. See Hunt (1998) supra note 139 at 442. See also Lester & Pannick (2000) supra note 137 at 383-384, who argue that this “diagonal” horizontal effect is beneficial as human rights principles will thereby be woven into the fabric of existing domestic law, so preserving the integrity of the domestic constitutional and legal order and promoting legal certainty.
contract of employment, which have in some cases recognised that this can be breached if fundamental human rights are infringed by the employer. For example, a Canadian arbitrator has decided that management prerogative does not extend to privacy-invasive random drug testing, the California Court of Appeal has stated that employers must respect human rights principles as part of the implied covenant of good faith and fair dealing, and the duty to exercise managerial discretion "fairly" under German labour law must be interpreted in light of constitutional human rights. Although it remains to be seen in practice how far the courts are prepared to extend this breach of contract argument, it is at least open to all employees, irrespective of whether they work for a public or a private body.

The HRA is also likely to have an influence on interpretation of unfair dismissal rights under the Employment Rights Act 1996, which provides that dismissal of an employee with more than one year's service (including a constructive dismissal) can be both substantively and procedurally unfair. The test is that of whether the employer's conduct was "reasonable" under section 98 of the Act. Relatively vague and flexible concepts such as "reasonableness" are clearly open to interpretation by courts and tribunals, which are now bound to interpret statutory provisions in line with human rights. The test of reasonableness applies both to whether any decision to dismiss the employee was reasonable, and to whether the disciplinary procedure was fair and reasonable in the circumstances. The court or tribunal must ask itself whether the employer acted within the "range of reasonable responses" of a reasonable employer. It seems unlikely that an employer who acts in breach of human rights could be found to have acted appropriately. This means that unjustifiable privacy-invasive employer practices are likely to render a dismissal unfair. For example, dismissal of

---

142 Re Canadian Pacific Ltd -v- United Transportation Union (1987), 31 L.A.C. 179 (Picher).
143 Luck -v- Southern Pacific Transportation Co. 267 Cal Repr 618 (CA 1st Dist. 1990) at 624 – 628.
145 As will be seen from the discussion of Canadian law in chapter three, application of human rights principles from the Charter has not in general had a significant impact on interpretation of the contract of employment.
146 Craig (1999) supra note 16 at 244.
147 The applicability of this test has been affirmed by the Court of Appeal in the cases of Madden -v- Midland Bank and Foley -v- Post Office, [2000] I.R.L.R. 827. It has also been argued that the HRA may actually require a move away from this relatively weak test where a human right is at stake; see Ford, M. (1998) supra note 122 at 47.
an employee for a reason connected with their private life could well be seen as an infringement of privacy and therefore unfair. In the specific context of electronic monitoring by employers, collection of evidence for disciplinary proceedings through surreptitious surveillance could make any consequent dismissal unfair on the basis of unreasonable disciplinary procedure. The potential is certainly there for the law relating to unfair dismissal to be developed in a way which is protective of workplace privacy rights.

The HRA will therefore be very significant for both public and private sector employers. A difference in treatment between employees of the two groups will remain, as only public sector employees can bring a direct claim for breach of the HRA. Employees of private bodies must base their claim on breach of another area of law to which human rights principles can be applied (generally requiring a dismissal or resignation, and so loss of employment), and those applying for a job to private employers appear to remain unprotected. However, the right to respect for private and family life will undoubtedly have an impact on all types of employer.

2.2.2 Application of the HRA to e-mail and internet monitoring

Having established that the right to privacy under the HRA can be relevant to both the public and the private sector workplace, can it be applied to the practice of e-mail and internet monitoring by employers?

The concepts of "private life" and "correspondence" have been relatively widely interpreted by the ECHR to include telephone conversations as well as written correspondence. Although to date there are no decisions concerning e-mail interception, by analogy it seems clear that this will also be covered by Article 8. Similarly, internet use involves use of a telecommunications system and could be seen as a private activity, making monitoring at least potentially a breach of privacy. In principle the right to respect for private life can therefore cover e-mail and internet monitoring. This gives the UK courts and tribunals scope

---

150 Supra note 148 at 245.
to develop the law in a way which is protective of worker privacy. However, will they do so? In particular, how far can these principles be taken in the specific context of the workplace?

To date, there is one decision of the ECHR which deals directly with the issue of electronic monitoring of employees in the workplace, *Halford v. United Kingdom*. The facts and reasoning of this case are worth considering in some detail, as it provides the only guidance available so far on these issues. It is particularly relevant to the development of UK law, as under the HRA courts and tribunals are specifically required to take decisions of the ECHR into account in interpreting *Convention* rights. The decision also gives some more general insights into approaches towards workplace privacy.

Alison Halford was an assistant chief constable within Merseyside Police, and in 1990 she brought an industrial tribunal claim alleging that failures to achieve further promotion were due to discrimination on the grounds of her sex. During the course of the sex discrimination proceedings, Halford claimed that a “campaign” had been waged against her by the Police Authority. This included an allegation that conversations over her office telephone relating to her tribunal claim had been intercepted by her employer in order to obtain information for use in the proceedings. This issue was raised before the Industrial Tribunal, which confirmed that there had not been a breach of the relevant statute, the *Interception of Communications Act 1985*, as this dealt only with public telecommunications networks. The Home Secretary similarly confirmed that the complaint did not fall within his responsibilities or the terms of the 1985 Act. Halford therefore applied to the European Commission of Human Rights alleging that various of her rights under the *Convention* had been infringed, including the right to respect for private life, and the case was referred to the ECHR for a decision.

The ECHR found that there had been a violation of Alison Halford’s right to respect for private life under Article 8 of the *Convention*. It held that telephone conversations made from business premises could be covered by the notions of “private life” and

---

153 Section 2(1).
“correspondence”, and that there was a reasonable likelihood that the calls made from her office at work had been intercepted. This infringement of the right could not be justified as it was not "in accordance with the law".\textsuperscript{154} The ECHR also found that the UK Government had violated Article 13 of the Convention by failing to provide an effective remedy for breach of Article 8 in these circumstances,\textsuperscript{155} because the Interception of Communications Act 1985 did not apply to internal systems such as that of the Merseyside Police.\textsuperscript{156} In consequence of these breaches of the Convention, Halford was awarded damages of £10,000.

This decision is certainly very significant. The case clearly establishes that the right to privacy under Article 8 is applicable to the workplace. It was found that Halford’s right to respect for her private life had been infringed in the context of telephone calls which had been made from the employer’s premises, in the employer’s time, and using the employer’s own telecommunications system and equipment. The Court was quite clear that in these circumstances Halford had a “reasonable expectation of privacy” in relation to telephone calls made from her office at work. By analogy, the same reasoning could be applied to e-mail and internet use in the workplace which utilises the employer’s time and equipment.

However, the decision itself is based on a very specific set of facts. The Court takes these various facts into account, but the explanation of its reasoning is brief, occupying only one paragraph of the judgement:

“There is no evidence of any warning having been given to Ms Halford, as a user of the internal telecommunications system operated at Merseyside Police headquarters, that calls made on that system would be liable to interception. She would, the Court considers, have had a reasonable expectation of privacy for such calls, which expectation was moreover reinforced by a number of factors. As Assistant Chief Constable she had sole use of her office where there were two telephones, one of which was specifically designated for her private use. Furthermore, she had been given the assurance, in response to a memorandum, that she could use her office telephones for the purposes of her sex discrimination case... for all of the above reasons, the Court concludes that telephone conversations made by Ms

\textsuperscript{154} This was on the basis that domestic law must provide some protection for individuals from secret surveillance and interception by public authorities, as established by the ECHR in Malone \textit{v- United Kingdom}, supra note 151.

\textsuperscript{155} \textit{Supra} note 151 at 477.

\textsuperscript{156} It is in partial response to this finding that the UK government has introduced the \textit{Regulation of Investigatory Powers Act 2000}, discussed further below.
Halford on her office telephones fell within the scope of the notions of "private life" and "correspondence" and that Article 8 was therefore applicable to this part of the complaint. 157

It can be seen that the Court considers a number of different factors in deciding that there was a "reasonable expectation of privacy" – lack of warnings, provision of private space, designation of a private telephone, and assurance that the telephone could be used for a private purpose. However, there is no indication as to the relative importance of these factors, whether these were essential or merely relevant considerations, and no suggestion of other factors which might be considered in different circumstances. This leaves the rationale for the finding somewhat unclear, and the Court fails to provide any explicit guidance to employers as to how to avoid infringements of Article 8. 158

It does appear that the fact that Halford was not warned of the possibility that her telephone calls might be intercepted was crucial to the Court's finding that she had a reasonable expectation of privacy. This factor is placed first in the Court's reasoning, and the other factors are viewed as reinforcing this expectation. This suggests that an employee's expectation of privacy can be destroyed if an employer simply tells employees that their telephone calls, or e-mail/internet use, may be monitored. This interpretation of the Court's reasoning is reinforced by the other factors, which similarly focus on the fact that the employer had led Halford to believe that her telephone calls were private. Halford effectively had a right to privacy because her employer allowed her to think that she had privacy. 159 It therefore appears arguable that the converse would also be true – if an employer makes it clear that such activities are not regarded as private, for example by implementing privacy-invasive policies and practices, any right of privacy in the workplace no longer exists as a result of simple exercise of management prerogative. As Ford has pointed out, there is a kind of "perverse logic" to the situation whereby the more workers are subject to intrusive surveillance, the more difficult it becomes to contend that they have a reasonable expectation of privacy. 160 As discussed in chapter one, 161 the values served by

157 Supra note 151 at 475.
158 Craig & Oliver (1998) supra note 141 at 51.
159 Ibid. at 55-56.
160 Ford, M. (1998) supra note 122 at 50. See also Study on the Uses and Misuses of Personal Data in Employer Employee Relationships (Personnel Policy Research Unit, 1999) (hereinafter "PPRU Study") at 30, which notes that the Halford case leaves many questions unanswered, and takes the view that it
privacy can be threatened by known pervasive surveillance, or even the expectation of being watched, as much as by covert monitoring. This interpretation of workplace expectations of privacy is something which also occurs in Canadian law, and the problems of an approach which gives the employer scope to define employee privacy rights are discussed in greater detail in chapter four.

The case also fails to give any guidance as to what interests might be advanced by an employer under Article 8(2) to justify infringements of worker privacy. As explained above, this was not considered by the ECHR because the employer’s activities were not seen as being “in accordance with law”, and therefore not even potentially justifiable. It is certainly possible that a wide range of employer interests could be put forward to justify monitoring of employees, such as those discussed in section 1.5 of chapter one, particularly under the category of “protection of the rights and freedoms of others”. Any such conduct by an employer would be subject to a proportionality test before the justification would be made out. Although there are no ECHR decisions directly on this point, the concept of proportionality in the context of worker privacy is also used under the DPA and Code of Practice (discussed further below). This suggests that considerations such as the availability of alternative means of achieving the same ends, use of the least intrusive practices possible, and openness by the employer, will all be relevant in deciding whether the employer’s actions were proportionate in the circumstances. However, development of the law under the HRA will turn on how the courts and tribunals choose to interpret these provisions. There is scope for employers to be subjected to a high level of scrutiny in justifying privacy-invasive practices, but similarly it is possible that employer’s business needs will be afforded deference by the courts. In any event, if an employer is able to prevent a “reasonable expectation of privacy” from arising in the first place, this stage is not even reached – if the employee has no right to privacy, the employer has nothing to justify.

Having pointed out these limitations, it is worth noting that the decision has already had an

---

161 Still appears lawful for an employer to record calls and access e-mail if these practices are incorporated into an employment contract and/or incorporated as an implied term under a company policy.

162 See sections 1.2.2, 1.3, and 1.4.2.
impact on guidance which has been produced on employee privacy over telephone calls at work. In March 1999, the Home Office issued a circular to Government departments which provided advice on the use and surveillance of electronic communications at work.\textsuperscript{163} This confirms the view that if an individual has been warned that calls might be monitored, this can remove any expectation of privacy. However, building on this circular, Oftel (the UK telephone industry regulator) has issued guidance to all companies which provide telephone services to employees.\textsuperscript{164} This takes the view that warnings alone will not necessarily remove employees’ expectation of privacy, because “...it is not reasonable to assume that people at work will never make or receive calls touching on personal or domestic matters.”\textsuperscript{165} The guidance goes on to recommend that staff should always be provided with some means of making private telephone calls from the workplace which will not be recorded or monitored, and employers should monitor other calls only where this is necessary and proportionate. Indeed, this guidance could be seen as going so far as to suggest that there is some kind of substantive right to make private telephone calls from work. By analogy, it could be argued that similar principles should be applied to e-mail and internet facilities in the workplace, even to the extent of providing a non-monitored computer or personal log facility for staff who wish to send and receive personal e-mails.\textsuperscript{166}

The right to respect for private life under the HRA undoubtedly has a direct impact on the issue of workplace e-mail and internet monitoring in the UK, and has already resulted in official guidance on interception of workplace telephone calls. It is difficult to predict at this stage exactly how the right will be developed by the courts. The \textit{Halford} case clearly establishes that the right to privacy can apply to use of the employer’s equipment during working hours. However, the ECHR’s reasoning is brief, and the case is of somewhat limited use because of the extreme nature of the employer’s conduct. It remains to be seen how far these principles can be extended. The decision also suggests that management

\textsuperscript{162} In any event, it is difficult to see how covert surveillance of an employee’s legally privileged conversations with her legal advisers could ever be justified under Article 8(2)!
\textsuperscript{163} \textit{Electronic Communications at Work – What you need to know}, HOC 15/1999 (Central IT Unit, Cabinet Office, 1999).
\textsuperscript{164} \textit{Recording Telephone Conversations on Private Networks} (Office of Telecommunications, 19 August 1999).
\textsuperscript{165} \textit{Ibid.} at paragraph 7. It is somewhat unclear how this fits with the interpretation suggested in the \textit{Halford} case that employers can define expectations of privacy in advance.
prerogative may be allowed to define an employee’s expectations of privacy.

2.3 The Regulation of Investigatory Powers Act 2000

RIPA relates directly to the issue of e-mail and internet monitoring by employers. Coming into force in 2000, the Act was introduced by the UK government for a number of reasons:167 concern about the enormous changes and expansion in the telecommunications sector; the need to update interception law to cover private networks, in order to give effect to the ECHR’s judgement in the Halford case; and in order to comply with the requirements of Directive 97/66/EC concerning privacy of telecommunications (“the Telecommunications Data Protection Directive”).168

RIPA itself is potentially very restrictive of employers who wish to monitor e-mail and internet use in the workplace. The Act provides that it is a criminal offence to intercept a communication in the course of transmission by either a public or a private telecommunication system.169 In relation to a private telecommunication system, an interception is excluded from criminal liability if it is made by or with the authority of the person with the right to control the operation or use of the system.170 This means that it is not a criminal offence for an employer to intercept e-mail or internet communications made using the employer’s own system. However, section 1(3) of the Act introduces a new type of civil liability for interceptions of communications over a private system, providing as follows:

“1(3) Any interception of a communication which is carried out at any place in the United Kingdom by, or with the express or implied consent of, a person having the right to control the operation or the use of a private telecommunication system shall be actionable at the suit or instance of the sender or recipient, or intended recipient, of

---

166 Jepson (1999) supra note 149 at 1675.
169 Sections 1(1) and 1(2).
170 Section 1(6).
the communication if it is without lawful authority and is either –

(a) an interception of that communication in the course of its transmission by means of that private system; or

(b) an interception of that communication in the course of its transmission, by means of a public telecommunication system, to or from apparatus comprised in that private telecommunication system.”

This effectively introduces a new privacy right into UK law, by creating tort of unlawful interception in the specific context of telecommunication systems. This new right applies to employer monitoring of telephone calls, e-mails and internet use, both on the employer’s own internal system and where that system is used to communicate with persons outside the workplace. Where an unlawful interception takes place, both the employee affected and any external sender/recipient of the communication can bring a claim.

It should be noted that the notion of “interception of a communication” under the Act does not include conduct relating to “traffic data”, including data identifying the person, apparatus or location to or from which the communication is transmitted. This means that not all forms of e-mail and internet monitoring are covered, even though other types of monitoring may also affect employee privacy. In particular, employers appear to be free to monitor information about where e-mails are being sent and from whom, and arguably also details of internet sites visited (if these are interpreted as a “location” from which a communication is sent). The Act is primarily designed to prevent interception and monitoring of the actual content of communications. Therefore some practices which are potentially invasive of employee privacy appear to be left unregulated by RIPA.

There are circumstances in which a potentially prohibited interception is lawful. In relation to employers, the first applicable provision is where both the sender and the recipient have consented to the interception of the communication, or the employer has reasonable grounds to believe that they have so consented. It is not clear from the Act whether the consent has to relate to interception of the specific communication in question, or whether more general

\begin{footnotes}
172 Section 2(9).
173 See further the discussion in section 1.4 of chapter one.
\end{footnotes}
consent to blanket monitoring and interception by the employer will be sufficient. In the case of interception of communications between employees within the workplace, it might be possible for an employer to argue that those employees had consented by agreeing to an employment contract or workplace policy which provided for such interceptions to take place – although it could also be questioned whether consent can be regarded as freely given in these circumstances, particularly if the alternative is dismissal or denial of employment. However, it is also possible that this provision will be more narrowly construed by the courts and limited to more specific consent. In any event, this argument would not apply where an employee is communicating with a person outside the workplace. It is often entirely impractical for an employer to obtain consent to interceptions from external third parties, and therefore this provision is at best of limited assistance to employers who wish to monitor e-mail and internet use.

However, the provision of most assistance to employers is the power provided by section 4(2) of the Act for the Secretary of State to make regulations authorising specific types of interception. This has resulted in the highly controversial Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ("the Lawful Business Practice Regulations"). These Regulations have watered down the restrictions placed on employer practices by RIPA to a large extent, in response to employer concerns. Indeed, in the context of e-mail and internet monitoring, it could be said that RIPA now hardly restricts employers at all. Consideration of the history of the drafting of the Regulations, in light of their final form, is illuminating in showing the UK Government's approach towards privacy in the workplace.

The Department of Trade and Industry initially issued draft regulations in July 2000, together

---

Section 3(1).


Ibid.

SI 2000 No 2699.
with a public consultation paper ("the DTI Consultation Paper").\textsuperscript{178} The draft provided that it would be lawful to monitor or keep a record of business communications for the purposes of national security, prevention or detection of crime, investigation or detection of unauthorised use of a telecommunication system, or in order to provide evidence of communications to establish the existence of facts or ascertain compliance with practices or procedures relevant to the business.\textsuperscript{179} This could only be done if reasonable efforts had been made to inform every person making or receiving the communication that it might be intercepted, or if there were reasonable grounds to believe that such persons were aware of the possibility of interception. All other interceptions would require the consent of both the sender and the recipient, in accordance with RIPA.

These draft regulations were based closely on the provisions of the Telecommunications Data Protection Directive. This Directive is primarily designed to control the activities of providers of public telecommunications networks. However, Article 5(1) of the Directive requires Member States to safeguard the confidentiality of all communications made over a public telecommunications network, and specifically prohibits interception and surveillance.\textsuperscript{180} This would include employer surveillance of employee communications which use a public network, namely any communications which are sent or received outside the employer's own internal system (although not monitoring of purely internal communications). Article 5(2) of the Directive provides an exception for, "any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication". Article 14(1) provides further exceptions for "national security, defence, public security, the prevention, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system".

\textsuperscript{178} DTI Public Consultation Exercise – Draft Regulations on Lawful Business Practice regarding the Interception of Communications (Department of Trade and Industry Communication and Information Industries Directorate, 27 July 2000).
\textsuperscript{179} Draft Regulation 3(1).
\textsuperscript{180} Article 5(1) reads as follows: "Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds
These specific exemptions were incorporated into the draft regulations. The DTI Consultation Paper makes it clear that the regulations were drafted in compliance with the Directive, with the additional aim of protecting purely internal communications (in compliance with the *Convention*). It should be noted that the wording of Article 5(2) was not followed exactly in the draft regulations, which allow interception of business communications, "in order to provide evidence of the communications for the purposes of either establishing the existence of facts or ascertaining compliance with practices or procedures relevant to the business...". It could be argued that this is somewhat wider than the purpose of providing evidence of a commercial transaction or other business communication set out in Article 5(2) of the Directive, which seems to be aimed at recordings made solely in order to prove the content of a commercial transaction or agreement. The wording of the draft regulations could be interpreted to include monitoring of employees to check compliance with internal practices, such as policies on harassment or use of e-mail, which does not appear to be contemplated by the Directive. It should also be noted that the Directive allows "recording" of communications only, while the draft regulations refer to "monitoring" of communications as well. However, overall the approach of the DTI Consultation Paper and draft regulations appeared to be within the spirit of the Directive. It is expressly stated that the regulations do not authorise interceptions for non-evidential purposes such as staff training, quality control and market research. The DTI Consultation Paper also confirms that the aim is to protect personal privacy, and appears to recognise the need for proportionality by stating that the intention of the legislation is to, "authorise the interception of communications without consent only when there are powerful arguments that the collection of evidence should be considered more important than confidentiality or privacy." This emphasises the fact that privacy is important, and should be overridden only when there are compelling reasons for doing so.

---

181 Supra note 178 at paragraphs 4 to 11.
182 Draft Regulation 3(1)(a)(iv).
183 Although the examples given at paragraph 14(a) of the Consultation Paper, *supra* note 178, are limited to compliance with regulatory practices and procedures, audit, debt recovery and dispute resolution.
The business response to the draft regulations was hostile, to the extent that the consultation period was extended until 15 September 2000 on the basis of employer concerns that they would not be able to monitor for legitimate purposes employees’ use of e-mail and the internet. The UK Government published a response to the consultation in October 2000, together with the final draft of the Lawful Business Practice Regulations. This response confirmed that, “The majority of responses [to the consultation] represented business interests and focused on the need to facilitate legitimate business activities.” The final version of the Regulations contains a number of additions and amendments to the original draft, all of which are aimed at accommodating business concerns about limitations on the ability to monitor and record communications. In the context of workplace monitoring by employers, the changes can be summarised as follows.

Firstly, monitoring or recording of communications is allowed in order to, “ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties.” This provision was added in response to concerns that businesses needed to be able to monitor calls for quality control purposes. Despite having initially rejected this approach, the Government decided that it would not be “in the interests of businesses or consumers” to require consent before quality control monitoring could take place, and amended the Regulations accordingly to allow monitoring for purposes such as staff training.

Secondly, the Regulations now allow monitoring or recording to be undertaken in order to secure or as an inherent part of the “effective operation” of the telecommunications system. This amendment, again made in response to business concerns, is designed to allow interception without consent for purposes such as protection against viruses and routing of e-mail traffic.

---

186 Lawful Business Practice Regulations – Response to Consultation (Department of Trade and Industry Communication and Information Industries Directorate, October 2000).
187 Ibid. at paragraph 11.
188 Regulation 3(1)(a)(i)(cc).
189 Supra note 186 at paragraph 18.
190 Regulation 3(1)(a)(v).
Thirdly, monitoring (although not recording) of communications is permitted, "for the purpose of determining whether they are communications relevant to the system controller’s business". Businesses had expressed particular concerns that they needed to be able to check voicemail systems and e-mail accounts in the absence of staff, without requiring prior consent. The Regulations were therefore amended accordingly, the Government expressing the view that this would, "achieve a balance between giving businesses free access to their own communications and protecting the privacy of non-business communications where these are permitted." It should be noted that the actual drafting of this new regulation is much wider than the specific purpose of allowing employers to check voicemail and e-mail during staff absences, seemingly allowing employers to monitor any communication at any time in order to check whether or not it is a business communication. However, this exception is limited to communications intended to be received by the person using the telecommunication system in question. Therefore it appears that employers can check incoming but not outgoing communications under this provision.

Businesses had also made representations about the need to intercept communications to check for unauthorised use of the system, such as monitoring of internet use to check for offensive material, or scanning of e-mails for indications of harassment or abuse. The Government confirmed that in fact this had already been covered by the provision allowing interceptions in order to investigate or detect unauthorised use of the system, and so businesses would be able to check that staff were not using the system for inappropriate purposes. It should be noted that the definition of "unauthorised" use is left entirely to the employer, and once the concept has been defined as widely as the employer thinks necessary, the power to monitor for this purpose is unconstrained.

Finally, a couple of provisions in the original draft regulations have been removed. In response to concerns about the practicality of informing third parties about possible

---

191 Supra note 186 at paragraph 13.
192 Regulation 3(1)(b).
193 Supra note 186 at paragraph 15.
194 Regulation 3(2)(d)(ii).
195 Supra note 186 at paragraph 23.
196 Ibid. at paragraph 24.
interceptions, businesses now only have to make "all reasonable efforts" to inform users of their own system that interceptions might take place. This means that employers still have to attempt to inform employees but not external third parties of any monitoring and/or recording of communications. The reference to provision of "evidence" of communications has also been removed from Regulation 3(1)(a), so that this is no longer required before an interception can take place for the purposes of establishing facts or ascertaining compliance with practices or procedures. This change is not referred to by the Government in its response to the consultation. However, the effect of this omission is to move the Regulations further from the wording of Article 5(2) of the Telecommunications Data Protection Directive, which as explained above provides only a limited exception for recording in order to provide evidence of commercial transactions or business communications.

These various amendments to the original draft regulations bring a much wider range of employer recording and monitoring activities within the scope of the exceptions to the requirement to obtain consent. All of the changes appear to have been made in favour of businesses, although as part of the consultation process the Government did receive representations on behalf of employees and consumers as well. The final version of the Lawful Business Practice Regulations has been received with disappointment by employees' organisations, and has been criticised as being a "snooper's charter". The Regulations certainly appear to allow employers wide scope to monitor and record telephone, e-mail and internet communications of their employees without consent, whether these are internal communications or with third parties outside the business. Permissible practices appear to include interceptions for the purposes of quality control, discipline, checking for harassment, checking for pornographic or other inappropriate material, and monitoring of whether

---

197 Morris (2001) supra note 175 at 63.
198 Supra note 186 at paragraph 11. No details are given of what these representations were, or why they do not appear to have influenced the drafting process.
199 For example, the Trades Union Congress has criticised the regulations for appearing to give employers, "...the right to monitor and record e-mails, telephone calls and internet interactions at work, almost without restriction and with no duty to consult or negotiate with trade unions or worker representatives." (Surveillance at Work: sensible solutions (Trades Union Congress, November 2000) at 3).
200 See for example, "Bosses get the go-ahead to eavesdrop on staff e-mails" (Daily Mail (London), 4 October 2000); "Bosses given right to spy on e-mails" (The Times (London), 4 October 2000).
incoming communications are relevant to the business or personal.\textsuperscript{201} Indeed, it is difficult to think of any potentially legitimate employer reason for intercepting communications which is not permitted by the Regulations.\textsuperscript{202} Interceptions are limited by Regulation 3(2)(a) to purposes relevant to the system controller’s business. However, all of the above types of monitoring are at least arguably relevant to the employer’s business, and in any event the Government’s own response to the consultation process envisages interceptions for these kinds of purposes. Even a communication which is clearly private could well be seen as relevant to the business if there is suspicion that the communication is in breach of company policy.\textsuperscript{203} The employer’s only obligation is to have made “reasonable efforts” to inform its employees that interception may take place. This could seemingly be done by the employer issuing a simple workplace policy or statement notifying employees generally that telephone calls, e-mails and internet use might be subject to interception.

The fact that employers’ needs to monitor communications are accommodated by the Regulations is not in itself necessarily a bad thing. As discussed in section 1.5 of chapter one, employers have a number of legitimate reasons for wanting to monitor e-mail and internet use in the workplace. Privacy has costs, and these must be recognised – it is a question of balance rather than privacy being an overriding value in all cases. However, a concern about the Regulations is the fact that they appear to give clear priority to business interests, at the expense of any meaningful right to privacy. The ability to record and monitor communications without consent is ostensibly limited to specific purposes. However, not only are these purposes potentially very wide, but the interception in question only needs to have been motivated by such a purpose. If an interception results in the employer obtaining personal information about an employee which is unrelated to the purpose of the monitoring, there appears to be no control over whether the employer is nevertheless entitled to collect and use that information - the interception is authorised by the legislation so long as it was originally carried out for a reason contemplated by the

\textsuperscript{201} All of which are justifications commonly put forward by employers in defence of monitoring practices, as discussed further in section 1.5 of chapter one.

\textsuperscript{202} Trades Union Spokesperson Lucy Anderson has been quoted as stating, “The government has defined particular circumstances when employers can intercept electronic information, but it is hard to think of anything employers might do that is not covered by the regulations.” (The Guardian (London), 25 November 2000).
Regulations. There is no recognition of the danger to employee privacy which may be caused by monitoring for legitimate reasons which unintentionally picks up other personal information as a “side effect” of the process.\textsuperscript{204}

This problem is exacerbated by the fact that the legislation does not include a principle of proportionality, requiring the reasons for interception without consent to be balanced against the potential effects on employee privacy. If an employer can establish that an interception was genuinely made for one of the purposes set out in the Regulations, it does not matter how compelling that purpose actually is, or how serious an invasion of privacy is involved – the interception is simply allowed anyway. This hardly seems to be furthering the aim of allowing privacy to be invaded only if there are “powerful arguments” that collection of evidence without consent is more important, as was claimed to be the primary purpose of the legislation in the DTI Consultation Paper.\textsuperscript{205} The possibility of including a proportionality test as part of the Lawful Business Practice Regulations was considered as part of the consultation process. However, this was rejected by the Government, who stated that they were, “…not convinced that this approach would lead to transparent or workable regulations. It would leave businesses and others unsure as to what interceptions activities were permitted. This would place businesses in a vulnerable legal position and might encourage some to relocate operations outside the UK.”\textsuperscript{206} Again, this approach gives business interests priority over the protection of privacy. The Government’s conclusion to its response to the consultation process states that the Lawful Business Practice Regulations would allow businesses to maximise the advantages of working with electronic communications, but be consistent with a “high degree of privacy” for users of the communications services.\textsuperscript{207} Taking into account the wide range of purposes which can justify monitoring without consent, the lack of protection of personal information collected as a side-effect of such interceptions, and the failure to include a principle of proportionality, this statement appears to be somewhat inaccurate.

\textsuperscript{203} See IDS Brief 672, November 2000, at 17.
\textsuperscript{204} See further section 1.4.2 of chapter one.
\textsuperscript{205} \textit{Supra} note 178 at paragraph 28.
\textsuperscript{206} \textit{Supra} note 186 at paragraph 37.
RIPA and the Lawful Business Practice Regulations have been received with some dismay by many in the UK because they do not fit with the other legislation which is relevant to the issue of e-mail and internet monitoring in the workplace. Indeed, the legislation appears to be contradictory, leaving employers and employees alike uncertain as to their rights and obligations. In relation to compliance with the provisions of the HRA, as explained above it is unclear as yet exactly when an employee will have a “reasonable expectation of privacy”, and which employer interests can be balanced against such a privacy right if it exists. It might therefore be arguable that an employer’s duty under the Regulations to make “reasonable efforts” to inform those potentially affected of the possibility of interception would prevent an expectation of privacy from arising in the first place, particularly in light of the emphasis placed on the lack of any warning in the Halford case. However, the concept of proportionality is central to the HRA but missing from the Regulations, and some of the permissible reasons for monitoring in the Regulations (such as to determine whether communications relate to the employer’s business) would appear to allow interceptions of private communications even where such communications as permitted by the employer.

It is certainly possible that the Lawful Business Practice Regulations could be challenged under the HRA for failing to provide sufficient protection of the right to respect for private life and correspondence. It is also worth noting that the Regulations will need to be interpreted by courts and tribunals in accordance with the right to privacy under the HRA, so it is possible that some of the provisions may accordingly be interpreted more narrowly than the Government has intended.

The Regulations are also inconsistent with the provisions of the DPA, which similarly includes a principle of proportionality in relation to the obtaining, recording and processing of personal data. This inconsistency has been exacerbated by the publication by the Information Commissioner of a draft Code of Practice on the use of personal data in

207 Ibid. at paragraph 45.
209 Morris (2001) supra note 175 at 63.
210 The Government recognised this inconsistency in its response to the consultation process (supra note 186 at paragraph 38), but took the view that the DPA would be sufficient to ensure that businesses acted in a proportionate manner – so failing to take into account the confusion which would be caused by the conflicting approaches in the legislation.
employer/employee relationships (discussed further below),\textsuperscript{211} which is very clearly at odds with the approach of the Regulations.

Finally, it is questionable as to whether RIPA and the Lawful Business Practice Regulations have implemented the provisions of the Telecommunications Data Protection Directive appropriately. In particular, as explained above, the exception to the requirement of consent envisaged by Article 5(2) of the Directive appears to be somewhat narrower than the exceptions contained in the Regulations. This is particularly the case now that any reference to the collection of "evidence" has been removed from the Regulations, together with the addition of some new exceptions which do not appear to fit within the terms of the Directive at all. It is therefore possible that the legislation could be challenged for failing to transpose fully the requirements of the Directive.\textsuperscript{212}

The Trades Union Congress have summarised the problems with RIPA and the Lawful Business Practice Regulations by stating that:

``An uncertain legal framework on surveillance which fails to balance employer and worker concerns and which cannot take account of individual workplace circumstances cannot be in the best interests of either employers or workers.''

Certainly the present state of confusion in the law is undesirable. It may be of assistance to turn to the provisions of the DPA, to see if a more coherent approach towards workplace monitoring is emerging through this route.

\textsuperscript{211} Draft Code of Practice - The use of personal data in employer employee relationships (Information Commissioner, October 2000).

\textsuperscript{212} European Directives take priority over inconsistent domestic laws. Emanations of the state (ie public bodies) can be sued directly for any breach of sufficiently clear provisions of a directive, known as "direct effect" (\textit{Van Dyne v. Home Office (No 2)}, [1974] E.C.R. 1537). Directives may also have "indirect effect", on the basis that courts have a duty to interpret UK statutes in line with the requirements of a directive wherever possible (\textit{von Colson and Kamann v. Land Nordrhein-Westfalen}, [1984] E.C.R. 1891, and see \textit{Webb v. EMO Air Cargo Limited}, [1993] I.C.R. 175 for application of this principle by the UK courts). If any inconsistencies can not be removed by judicial interpretation, the state itself can also be sued for failure to implement a directive by individuals who have suffered consequential loss (\textit{Francovich v. Italian Republic}, [1991] E.C.R. I-5357).

\textsuperscript{213} Trades Union Congress (2000) supra note 199 at 10.
2.4 The Data Protection Act 1998

The DPA is the other major piece of legislation which relates directly to the issue of employee privacy and e-mail/internet monitoring, and it is therefore helpful to consider this in some detail. Its provisions are important both in themselves and in the way in which they interrelate with the HRA and RIPA. Overall, a more privacy-protective approach is taken towards electronic monitoring in the workplace than that taken by the legislation and guidance discussed so far, although it will be seen that in some respects deference is still afforded to employer interests at the expense of employee privacy.

2.4.1 Application of the Data Protection Act to e-mail and internet monitoring

The DPA was drafted in order to implement the provisions of European Directive 95/46/EC ("the Data Protection Directive"), which deals expressly with the issue of the processing of personal data.\(^{214}\) It builds on the provisions of the Data Protection Act 1984, which dealt solely with certain types of processing of automated data. The DPA controls the "processing" of "personal data" by any "data controller". The concept of "processing" is defined as "obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data".\(^{215}\) "Personal data" is defined as data relating to a living individual who can be identified from those data.\(^{216}\) These definitions are clearly wide enough to include the obtaining of personal information by means of electronic monitoring such as interception of e-mail or monitoring of internet use, and the DPA is therefore directly relevant to the issues under discussion.

The DPA deals with the rights of individuals to have access to data held about them, to prevent certain types of processing, and to rectify, block and erase inaccurate data (Part II of the Act), and also with the requirement for data controllers to register with or notify the Information Commissioner about processing of data (Part III of the Act). However, the

\(^{214}\) Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

\(^{215}\) Section 1(1).

\(^{216}\) Ibid.
provisions which are most directly relevant to the issue of electronic monitoring are those dealing with the “data protection principles” and preconditions to processing contained in Schedules 1 to 3 of the Act.

Section 4(4) of the DPA specifies that, “it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller.” This is the key provision of the Act with respect to protection of privacy, as it results in limitations being placed on the ability of employers to process personal data about their employees. The central restriction on the activities of data controllers is the requirement that personal data be processed “fairly and lawfully”. This requires that at least one of the conditions set out in Schedule 2 is met in relation to the processing, a number of which are potentially applicable in the context of electronic monitoring by employers.

Firstly, processing will be lawful if the data subject has given “consent”. This obviously requires the individual affected by the monitoring to have agreed that it should take place, rather than simply having been warned of the possibility as is required under the Lawful Business Practice Regulations (and arguably under the HRA in relation to whether there is a reasonable expectation of privacy). However, there is a question as to what constitutes meaningful “consent” in the context of an employment relationship. If employee consent can be taken from simple agreement to a contract of employment or workplace policy which provides the employer with a general power to carry out monitoring, then in practice this is no different from a warning that monitoring might take place. In light of the inequality of bargaining power which many see as inherent in the relationship between employer and employee, the individual in fact has no real choice as to whether to agree to the monitoring.

217 It is worth noting that the Data Protection Directive is much more explicit that this is the main purpose of the legislation. Article 1(1) of the Directive states that the object is to, “protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.” The restrictions on processing are the first substantive provisions in the Directive, at Articles 6 to 8, and are clearly central to the purposes of the legislation. In contrast, the DPA fails to mention the concept of “privacy” anywhere in its wording, and the restrictions on processing are set out in Schedules at the end of the Act. The provisions themselves do follow the requirements of the Directive fairly closely, although with a few significant alterations.

218 Schedule 1 Part I paragraph 1.

219 Schedule 2 paragraph 1.
The theme of consent to ostensibly privacy-invasive practices also appears in Canadian law, and the extent to which it is appropriate to apply such a principle in the context of the employment relationship is discussed in more detail in section 4.2.2 of chapter four. This is particularly relevant in light of the wording of the Data Protection Directive, which treats the issue of consent in rather more detail. Consent is defined as, "any freely given specific and informed indication of [the data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed". This would seem to require an individual to be told exactly why and how personal data was being processed before consent would be taken as having been given, and so limit to some extent the ability of employers to obtain consent to very general monitoring practices. The requirement that consent be "freely given" could also arguably limit the ability of employers to obtain "agreement" from employees in circumstances of unequal bargaining power, at least in the context of introduction of a new workplace policy which employees would otherwise be taken to have accepted by implication. In relation to consent as a precondition to processing, the Directive further requires that this has been given "unambiguously". Again, this would seem to prevent employers from arguing that privacy invasive practices had been accepted by implied consent, and also prevent employers from obtaining agreement to very vague and general monitoring powers. It is interesting that the DPA has not included these provisions. The omission of the requirement for "unambiguous" consent seems particularly significant, and suggests that the DPA is therefore designed to allow practices which would otherwise be prevented.

Processing can also take place if it is "necessary" for the "performance of a contract to which the data subject is a party." This wording is reproduced from the Directive. In the employment context, it is possible that an employer could argue that electronic monitoring is necessary for proper performance of the contract – for example, surveillance for purposes of

220 Article 2(h).
221 Article 7(a).
222 Craig (1999) supra note 16 at 254.
223 As well as raising the possibility that the UK has failed to implement the Directive properly. See supra note 212 for an explanation of the possible consequences.
224 Schedule 2 paragraph 2.
quality control, to check that employees are performing their jobs correctly. However, it is questionable whether such practices would really be "necessary" for performance of the contract, and therefore it is likely that this provision will not be of much assistance to employers. Perhaps more relevant is the provision allowing processing to take place if it is, "necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract." This could potentially be used to justify monitoring for a number of purposes. For example, monitoring of e-mail in order to catch the perpetrator of harassment could be justified on the basis of the employer's obligation to prevent discrimination in the workplace, and a similar argument would apply to monitoring of internet use in order to prevent the distribution of pornographic material. Again, the processing would need to be "necessary" for this purpose. However, if the employer could show that alternative methods would not achieve the desired aim, this provision of the DPA does seem to assist the employer who wishes to monitor e-mail and internet use in order to comply with genuine legal obligations.

Even if these conditions do not apply, there is an alternative provision which may be applicable. Paragraph 6(1) of Schedule 2 provides that the processing can take place if it is, "necessary for the purposes of legitimate interests pursued by the data controller...except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject." This effectively provides a proportionality test, allowing monitoring by an employer where this is for good reason and does not unduly infringe the employee's rights. This balancing of interests is something which was expressly rejected by the Government in the context of RIPA and the Lawful Business Practice Regulations (as discussed above). However, the balancing itself appears to be weighted markedly in the employer's favour. So long as the employer has a "legitimate interest" which is being pursued, monitoring will only be prevented if the damage to the employee's interests is "unwarranted". This is in contrast to the wording of the Directive, which provides that processing is not allowed if the data controller's legitimate interests are, "overridden by the interests or fundamental rights and freedoms of the data subject".

Craig (1999) supra note 16 at 255.
Schedule 2 paragraph 3.
Article 7(f).
approach of the Directive is a more traditional proportionality test, where the question is one of which right or interest can override the other. The DPA’s requirement that processing be “unwarranted” seems to set up a stricter test, in the data controller’s favour. Indeed, unless the intention was to change the meaning, it is difficult to see why the wording of the Directive has been departed from at all. Of course, it remains to be seen how this provision will be applied in practice. The HRA also uses a proportionality test in the context of justification of infringement of rights, including the right to respect for private life. As discussed above, courts and tribunals do have a duty to interpret legislation in accordance with the HRA where possible. It is therefore possible that this provision of the DPA will be interpreted in the same way as the HRA proportionality test, requiring a more equal balancing of the importance of the employer’s interests against the seriousness of the impact on the individual’s rights. However, the drafting of the DPA itself suggests that the data controller’s interests are being given more protection than the individual’s right to privacy.

The DPA does contain other provisions which are based to some extent around the concept of proportionality, which may in themselves help to ensure that processing only takes place where really necessary. In addition to the requirement that data be processed fairly and lawfully, the DPA also requires that data should only be obtained and processed for “specified and lawful purposes”, and also that data should be “adequate, relevant and not excessive” in relation to those purposes. The limitation to collection for specified purposes would seem to prevent employers from keeping and using personal information which was discovered as a side-effect of monitoring for other purposes. The requirement that data be relevant and not excessive in relation to specific purposes could also be interpreted as requiring employers to use the least intrusive means possible to achieve their aims, for example by using specifically targeted rather than blanket monitoring in the workplace.

228 Craig (1999) supra note 16 at 256.
229 See Ford, M. (1998) supra note 122 at 36, who notes that this provision will only work if the courts are prepared to recognise the fundamental importance of human rights, and not equate legitimate interests with economic interests.
230 Schedule 1 Part I paragraph 2.
231 Schedule 1 Part I paragraph 3.
The DPA also contains some further provisions which would appear to prevent covert surveillance and monitoring in the majority of cases. In relation to whether processing is fair and lawful, account must be taken of the method by which data is obtained, including whether any person has been "deceived or misled". This would seem to rule out covert monitoring, as well as preventing the collection of personal information if the individual had understood processing to be taking place for other reasons. The subject of data processing is also entitled to be given information about the identity of the data controller, the purposes for which the data are to be processed, and any further information which is necessary to make the processing fair – this is to be done at the time when the data is first processed, or as soon as practicable thereafter. Again, this prevents covert monitoring by employers. It also ensures that individuals are made aware of the fact that monitoring is taking place, imposing a somewhat higher standard than the requirement to make "reasonable efforts" to warn of monitoring which is imposed by the Lawful Business Practice Regulations. There is an exception to this requirement if provision of this information would involve a "disproportionate effort", but it is difficult to see how this would be applicable in the workplace context. There is also one further exception to the requirement of fairness, where personal data is being processed for the purposes of the prevention or detection of crime. This suggests that employers would be able to carry out covert monitoring to prevent or detect fraud or theft, or to prevent illegal material from being circulated by e-mail or over the internet. However, overall these provisions would seem to require employers to be open with their employees about the fact that monitoring is taking place, and the reasons why this is being done. The need to give specific information about the purposes of data collection again imposes a higher duty than that envisaged by RIPA and the Lawful Business Practice Regulations.

---

232 Schedule I Part II paragraph 1(1).
233 Schedule I Part II paragraph 2(1)(b).
234 Schedule I Part II paragraph 3(2)(a).
235 Section 29.
236 Employers will also need to be particularly careful about the additional protections provided by the DPA for "sensitive" personal data, which includes information about an individual's racial/ethnic origins, political opinions, religious beliefs, trade union membership, health, sexual life, and criminal activities (Section 2). Processing of sensitive data is subject to more restrictive conditions, set out in Schedule 3 of the Act. In relation to consent, this will only allow processing to take place if it is "explicit" consent (Schedule 3 paragraph 1). In addition, the alternative proportionality test which is available in other cases does not apply to processing of sensitive data.
2.4.2 The Draft Code of Practice

The Information Commissioner has built on the provisions of the DPA in the specific context of the workplace by producing a draft code of practice on the use of personal data in employer/employee relationships ("the Draft Code")\(^\text{237}\), in accordance with her powers under section 51(3)(b) of the DPA. The Draft Code includes consideration of monitoring of employee communications. Overall, the Information Commissioner has interpreted the provisions of the DPA in such a way as to provide genuine protection of worker privacy, although still recognising that employer monitoring may be justified for specific reasons. The Draft Code has been the subject of public consultation, and has been open to some criticism on the basis of its inconsistency with the provisions of RIPA. Publication in its final form has now been delayed until the end of 2001.\(^\text{238}\)

The Draft Code, in contrast to the DPA, expressly recognises that workplace monitoring potentially impacts on employees' privacy and autonomy. The phrase "autonomy" is used in addition to "privacy" in order to, "...make it clear that it is not only an employee's right not to have information about his/her private life or behaviour widely known that is important. An employee's right to expect a degree of trust from his/her employer, and be given reasonable freedom to determine his/her own actions without constantly being watched or asked to explain, must also be respected."\(^\text{239}\) This takes a relatively wide approach towards defining the rights of employees which need to be respected, recognising the various values such as individual autonomy and dignity which are served by protection of privacy.\(^\text{240}\) The Draft Code also recognises that monitoring of business as well as personal communications might affect privacy or autonomy, if processing of personal data is involved - for example, where personal reasons for postponing a business meeting are intended to be revealed only to a particular recipient.\(^\text{241}\)

\(^{237}\) *Supra* note 211.

\(^{238}\) *Supra* note 211 at paragraph 6.1.

\(^{239}\) *Supra* note 211 at paragraph 6.3.

\(^{240}\) The various valued served by privacy are discussed further in section 1.2.2 of chapter one.

\(^{241}\) *Supra* note 211 at paragraph 6.3.
The Draft Code emphasises the requirement of proportionality throughout, which is seen as key to whether processing is “fair and lawful” under the DPA. The overall principle is that, “any intrusion on an employee’s privacy or autonomy should be in proportion to the benefits of the monitoring to a reasonable employer.” Application of this principle gives general standards for monitoring, including the principles that: monitoring should not be introduced if the adverse impact is out of proportion to the benefits; if comparable benefits can reasonably be achieved by a method with less impact, then this method should be adopted; and monitoring should be specifically targeted on areas where it is necessary and proportionate to achieving the relevant business purpose. The Draft Code then goes on to apply these principles to the specific questions of e-mail, internet and telephone monitoring. In relation to e-mail monitoring, it is emphasised that the mere fact it is easy for employers to monitor e-mails does not alter the need for proportionality. If monitoring is required, then the least intrusive method should be used – actual content should only be monitored if neither a record of traffic nor a record of the subject of e-mails would achieve the business purpose in question. In relation to monitoring for the purposes of virus detection, this should be done by automatic means, and would never warrant the actual reading of the content of incoming e-mails. A similar approach is taken towards internet monitoring – means such as restriction of access rather than monitoring should be used to enforce policies wherever possible, and monitoring of sites visited or content viewed should only be used if recording of the time spent on the internet would not achieve the employer’s purposes.

The Draft Code goes on to emphasise that employers should be realistic in identifying risks which allegedly can only be controlled by privacy-invasive monitoring. In the context of e-mail, it is noted that employers claim monitoring is necessary in order to prevent the loss of trade secrets. However, the Draft Code also points out that trade secrets can be communicated in other ways as well – unless there is evidence that e-mail poses a particular
risk in this respect, and monitoring is part of a wider package to tackle the problem, this argument would not justify routine monitoring. Some scepticism is also shown towards employer arguments in justification of internet monitoring. The Draft Code states that if monitoring is justified on the basis of prevention of criminal activity, there needs to be some evidence that this is actually taking place, and also notes that it is unlikely that employers could be prosecuted for employee activities carried out in disregard of the employer’s instructions. In relation to the causing of harassment or distress, this would not justify monitoring unless there is evidence that this is likely to take place and cause real distress or offence— it is noted that the mere causing of embarrassment could be dealt with in the same way as if an inappropriate magazine had been brought into the workplace.

The Draft Code’s approach towards proportionality is one which gives full weight to employee interests, and requires genuine and pressing justifications from employers for intrusive monitoring practices. Clearly this does not favour the employer’s interests in the way which seems to be indicated by the somewhat unbalanced proportionality test contained in Schedule 2 of the DPA. It is also clear that the provisions of the Draft Code are at odds with RIPA and the Lawful Business Practice Regulations. As discussed above, RIPA and the Regulations take an approach whereby monitoring can be justified so long as it is for one of the potentially wide purposes set out in the legislation, and there is no consideration of the importance of this purpose or the seriousness of the effect on privacy. In contrast, the Draft Code expressly limits employer practices to the least intrusive possible in the circumstances, even where the employer has important business reasons for monitoring, and goes so far as to question the genuineness of justifications which are commonly put forward for e-mail and internet monitoring.

The Draft Code also considers the issue of employer policies about e-mail and internet use and monitoring. As a general principle, employees should be made aware of monitoring and the purposes for which the information is being collected, except in exceptional circumstances. Covert monitoring of performance can never be justified, and covert

---

249 *Ibid.* at paragraph 6.3.3.
monitoring of behaviour should only take place in very limited circumstances.\textsuperscript{250} It is recommended that employers should have a policy on the use of electronic communications (although this is not actually required by the DPA). However, the Draft Code also recognises that the mere existence of a policy may not assist employers in showing that monitoring is fair and lawful. If a policy is not enforced, it is the actual practice rather than the policy which will be used in assessing whether monitoring is proportionate, and it is emphasised that employees should not be misled into false expectations of privacy by, for example, including a general contractual condition relating to monitoring but not actually carrying it out until a later date.\textsuperscript{251}

The Draft Code goes further than simply confirming that the actual application of workplace policies is relevant to proportionality. It is suggested that in some cases the mere fact that the employer has a workplace policy in place, or has warned of the possibility of monitoring, does not prevent the employee from having an enforceable right to privacy. In the context of monitoring of the content of e-mails, the Draft Code twice contains the statement, “Do not open e-mails that are clearly personal”.\textsuperscript{252} This suggests that an employee is entitled to maintain the privacy of clearly personal communications, even if the employer has a contractual term or policy which ostensibly allows monitoring of the content of all e-mails. Similarly, in relation to internet access monitoring, the Draft Code questions whether monitoring of content rather than time spent on the internet can be justified if employees are allowed to access the internet in their own time for private purposes.\textsuperscript{253} Again, it appears that potentially this can be unfair even if the employer had expressly reserved the right to carry out content checks.

This approach towards warnings and workplace policies is very different from that taken by RIPA, and also contrasts with the HRA. The Draft Code recognises that employers may legitimately have workplace rules which limit access to and use of e-mail and the internet. However, the DPA is not concerned with whether such rules are fair and reasonable, but

\textsuperscript{250}\textit{Ibid.} at paragraphs 6.1 and 6.2.
\textsuperscript{251}\textit{Ibid.} at paragraph 6.3.
\textsuperscript{252}\textit{Ibid.} at paragraph 6.3.2.
\textsuperscript{253}\textit{Ibid.} at paragraph 6.3.3.
rather with whether any monitoring carried out by the employer to enforce the rules is in compliance with the Act. This means that even if the employer has a blanket policy that prevents personal use of e-mail and the internet, together with a clear warning that all e-mail and internet communications might be monitored, the concept of proportionality under the DPA as interpreted in the Draft Code may still limit the scope of employers' monitoring practices. This is in stark contrast to the provisions of RIPA and the Lawful Business Practice Regulations, which allow monitoring for a wide range of purposes so long as "reasonable efforts" have been made to warn employees of this possibility. This approach towards proportionality is more in line with how the concept is interpreted and applied under the Convention, and therefore also with how the HRA is likely to be applied in practice. However, a different approach is taken as to when employees will have a "reasonable expectation of privacy". As discussed above, the Halford case suggests that any reasonable expectation of privacy under the HRA can be removed if the individual has been led to believe that communications are not private. If there is no expectation of privacy, the proportionality test is not reached at all. Under the Draft Code, although the employee's expectations may be relevant to whether or not monitoring is considered proportionate, the employee may have a right to privacy despite clear warnings that monitoring may take place. This in turn shows a rather different attitude towards the ability of employers to dictate their employees' rights and expectations by workplace contract or policy.

2.5 Conclusions

In summary, the present state of UK law in relation to workplace e-mail and internet monitoring is unclear and contradictory. Under the HRA, employee rights to privacy at work turn on whether there is a "reasonable expectation of privacy", and the test for when such an expectation will arise is as yet undeveloped. Under RIPA and the Lawful Business Practice Regulations, employers have wide scope to carry out monitoring for business reasons, so long as an attempt is made to warn employees that this may happen. Under the DPA, the concept of proportionality requires employers to minimise intrusions into worker privacy as

far as possible, irrespective of warnings, contracts or policies. It certainly appears that there is no one theory of privacy or the employer/employee relationship underlying the UK legislation.

The problems and inconsistencies in UK law will be considered further in the final chapters of the thesis, where they will be analysed as part of a wider discussion about the problems with applying the concept of information privacy within the context of an employment relationship. Despite the incoherence, it is possible to identify a trend in the law, namely a tendency to afford employer interests greater protection than employee interests. This is suggested by the *Halford* case, where employers are seemingly given the power to control the extent of privacy rights through application of the concept of "reasonable expectations" of privacy. Even more clearly, the drafting of the Lawful Business Practice Regulations shows considerable deference towards employer prerogatives to control the workplace, denying information privacy rights over e-mail and internet use altogether in circumstances where the employer has a business reason for carrying out monitoring. These issues will be explored in more depth in chapters four and five.

The next chapter deals with Canadian law on privacy and how this is applied to workplace e-mail and internet monitoring. It will be seen that, although Canada has a longer history of human rights protection than the UK, Canadian law also suffers from inconsistencies and other similar difficulties in applying information privacy principles within the workplace.
3 THE LAW IN CANADA

"...the increasing use of technology to monitor workers is another omen. With each new form of surveillance we become less like individuals and more like automatons, monitored for defects and aberrant behaviour that will consign us to the reject pile or mark us for 'corrective' measures." (Privacy Commissioner of Canada).\(^{255}\)

The concept of privacy has been present in Canadian law for a number of years, both in legislation and in judicial decisions. Legal protection of privacy rights is therefore more advanced than in the United Kingdom, where such issues are being considered seriously for the first time. However, Canada does not have a comprehensive privacy regime, either generally or with specific reference to the workplace. Instead, the law is a somewhat confusing mixture of various pieces of legislation, application of the Canadian Charter of Rights and Freedoms\(^{256}\) ("the Charter"), and specific application of privacy principles drawn from the Charter in court and arbitration decisions.

This chapter looks at the various ways in which privacy-invasive practices by employers, in particular e-mail and internet monitoring, may be restricted by Canadian law. This will involve consideration of existing and proposed legislation, Charter jurisprudence, and principles which have emerged from grievance arbitration decisions. Despite the various sources of legal protection, it is possible to discover some underlying themes which are being applied to the issue of workplace privacy.

3.1 Specific legislation relating to privacy

There are various pieces of Canadian legislation which relate directly to an individual’s right to privacy in different circumstances. However, it must be noted that this legislation does not provide one coherent approach. This is largely due to the complexities of the Canadian federal structure, whereby the federal government can legislate only on specific matters,

while other matters fall under the jurisdiction of the provincial governments. There are therefore some statutes enacted by the federal government which apply directly only to employees falling under federal jurisdiction. Various provinces have also enacted their own privacy legislation, while others have no specific legislation at all. The level of legal regulation of privacy-invasive practices in the workplace therefore depends on whether the employer is federally regulated, and in which province the employment is based. It may also depend on whether the employee works for the public or private sector. The different pieces of legislation also take differing approaches towards privacy, in a way which is somewhat similar to the conflicting approaches of the new UK legislation.

The main legislative provisions which impact on privacy in the workplace can be summarised as follows.

3.1.1 The Criminal Code

The Criminal Code contains specific provisions relating to interception of communications. This is a federal statute, and applies throughout Canada. Section 184(1) makes it an offence to intercept a private communication:

"Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

(2) Subsection (1) does not apply to
(a) a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it...."

In principle, this makes it an offence for an employer to intercept an employee’s private communications from the workplace without consent. "Intercept" is defined widely, to include listening to, recording and acquiring a communication, and therefore would appear
to include monitoring of e-mail and internet use. At first sight, this seems to place a clear restriction on employers' activities. However, the extent to which the Criminal Code can be used to provide meaningful protection of employee privacy will depend on how the legislation is interpreted – in particular, what is a private communication, and what is meant by consent?

The concept of a “private communication” is defined as a communication, “made under circumstances in which it is reasonable for the originator thereof to expect that it will not be intercepted by any person other than the person intended by the originator thereof to receive it.”^{261} In the context of the workplace, there is a question as to when it would be “reasonable” for an employee to expect that use of e-mail or the internet would not be monitored. In particular, if the employer has a workplace policy making it clear that such communications might be intercepted, can an employee still claim to have expected that there would be no interception? This raises issues about the definition of an employee's “reasonable expectation of privacy”, and whether expectations can be set by employers simply asserting that workplace communications are not regarded as private. To date the Canadian courts have not been asked to apply the Criminal Code to a case of employer monitoring, and it therefore remains to be seen how an employee's expectations of privacy will be interpreted in this context. However, it certainly seems possible that an employer could avoid infringing the Criminal Code by leading employees to expect that all communications may be liable to interception, so making it “unreasonable” for them to have thought otherwise.

Liability under the Criminal Code can also be avoided if an employer has obtained “consent” to the interception. This concept is not defined further, although the consent can be either express or implied. In the context of the workplace, consent could be obtained through the employment contract, or by employees agreeing to a policy on electronic monitoring. Consent might even be implied from employee acquiescence to known monitoring practices.^{262} It is possible that the idea of consent may be interpreted more strictly by the

---

^{261} Ibid.

^{262} See further the discussion about consent in section 4.2.2 of chapter four.
courts – for example, the courts may be concerned with the precise type of monitoring which an employee has agreed to, and unwilling to accept blanket consent to a policy of general monitoring. However, to date there are no decisions in the jurisprudence on this point.

It is clear that the Criminal Code is not concerned with the reasons why an interception may be taking place. If an individual does not have an expectation of privacy, or if consent has been obtained, the interception can simply go ahead – there is certainly no consideration of proportionality, or requirement that the interests of the interceptor and the affected individual should be balanced against each other. Of course, it must be remembered that this is a criminal statute, and therefore such additional restrictions would not necessarily be appropriate. As a criminal statute, these provisions will also need to be interpreted in the manner most favourable to the accused, making it likely that "reasonable expectations" of privacy will be interpreted narrowly and "consent" will be interpreted widely. It should also be noted that the Criminal Code would be of somewhat limited use in providing a remedy for disgruntled employees, who might be able to threaten their employer with criminal liability, but could not use the statute to sue for compensation or obtain reinstatement. Because these provisions of the Criminal Code have not yet been applied to a case of workplace monitoring, in practice they do not appear to restrict employer activities. However, it can be said that prudent employers should perhaps consider obtaining employee consent to monitoring practices in order to be sure of avoiding criminal liability. An approach towards privacy which focuses on reasonable expectations and consent is also mirrored in other legislation and court decisions (discussed further below).

3.1.2 The Federal Privacy Act

The Privacy Act is a piece of federal legislation which regulates the collection and use of personal information by government institutions. Although the legislation might have been designed to protect citizens against governmental information gathering activities, in practice it can also be relied on directly by government employees, and this aspect of the legislation is

---

264 Ibid. at 878.
confirmed by the Privacy Commissioner of Canada's approach towards workplace privacy issues discussed further below. It is therefore directly relevant to electronic monitoring of employees of government institutions.

The Privacy Act relates to "personal information", which is defined as, "information about an identifiable individual that is recorded in any form...". This definition appears to be wide enough to include the content of e-mails and monitoring of internet use, where this reveals information about an individual. Such information cannot be collected by a government institution unless it, "relates directly to an operating program or activity of the institution." In the context of employer monitoring practices, this would certainly prevent the collection of personal information for no good reason. It may also restrict the reasons on which a government employer could rely to justify monitoring, if these were not related to the operation of the business. However, it is possible that this provision could be fairly widely interpreted, so that many of the reasons given for monitoring would be seen as relating to the institution's activities. For example, purposes such as protection of confidential information, prevention of illegal conduct, and even prevention of abuse of time and the employer's property, could all be seen in a broad sense as relating to the employer's activities. The Privacy Act also specifies that individuals must be informed of the purposes for which personal information is being collected, and such information can only be used consistently with that purpose. This means that electronic monitoring by employers which results in the collection of personal information must be open, and for specific purposes. The requirement that personal information be used only for specified purposes would also seem to prevent employers from relying on information collected as a side effect of monitoring originally carried out for different reasons.

---

266 Section 3.
267 Section 4.
268 Section 5(2).
269 Section 7.
270 Section 5(3)(b) does allow collection without informing the individual of the purposes where this would otherwise, "defeat the purpose or prejudice the use for which information is collected". This would seem to allow covert monitoring for purposes such as prevention of crime, detection of the perpetrators of harassment, and possibly even enforcement of an employer's policy about use of e-mail and the internet, although the employer would have to show why prior disclosure of the monitoring would prejudice these purposes.
271 One of the ways in which employers may gather personal information discussed in section 1.4.1 of chapter one.
The Privacy Act protects privacy through control of the purposes for which personal information can be collected, in a way which is similar to the approach of the DPA in the UK. This is very different from the Criminal Code, which protects privacy by requiring consent, but is unconcerned with the reasons for interception of communications. However, the Privacy Act is not as privacy protective as the DPA. It contains no additional preconditions to information collection, such as prior consent. Neither does it contain any principle of proportionality. Indeed, it appears that the "activity" of the institution to which the information relates does not even need to be a legitimate one, and the information needs only "relate" to this activity, rather than be necessary to it.272 The potential impact of the Act on workplace e-mail and internet monitoring is therefore somewhat limited.

The Privacy Act also created a federal agency to oversee the operation of the Act, the Privacy Commissioner of Canada ("the PCC"). The PCC has wide powers to consider complaints under the Act, and carry out investigations. Although the PCC does not have the actual power to adjudicate claims or issue legally binding opinions, he or she fulfils a conciliatory and advisory role in relation to government institutions, and produces an annual report on compliance with the Act and more general privacy-related issues.273 Over the years the PCC has received and dealt with a number of complaints relating to workplace privacy, including the issue of electronic monitoring by employers. Consideration of some of these opinions will help to show the extent to which the Privacy Act can be used to regulate the monitoring of e-mail and internet use.

In the PCC’s Annual Report for 1993-94, there is a report about a complaint made against the Royal Mint, relating to monitoring of employees’ telephone calls. The Royal Mint implemented telephone monitoring for "training and performance evaluation purposes", and

---

272 Craig (1999) supra note 16 at 124.
273 The PCC is an independent ombudsman who acts as an advocate for the privacy rights of Canadians, reporting directly to Parliament. The PCC’s full powers are to investigate complaints and conduct audits in accordance with the two relevant federal laws (the Privacy Act and PIPEDA), publish information, take matters to the Federal Court of Canada, carry out research into privacy issues, and to promote public awareness and understanding of privacy.
informed employees about this new policy three days in advance of its implementation. The PCC's opinion conceded that the collection of personal information for the purposes of employee assessment did not contravene the Act, in light of the fact that the employees were informed in advance. Although not made clear in the opinion, it appears that this purpose was seen as relating to an activity of the institution, and therefore permitted – the Act does not require any consideration of the importance of this purpose, or whether it could be achieved by other less intrusive means.

The PCC's Annual Report for 1995-96 contains a complaint relating specifically to the issue of e-mail interception. An employee of the Correctional Service Canada complained that her e-mail had been accessed by her supervisor during her absence from work. This was done by the employer in order to obtain a copy of an important document. The PCC found that this was not a valid complaint. This conclusion is perhaps unsurprising, in light of the fact that the information was not of a personal nature, and was accessed for a good reason. However, perhaps more surprising is the general attitude expressed towards workplace e-mail. The PCC expressed the opinion that:

"Managers and employees alike should remember that e-mail is not secure, and even deleted e-mail messages can sometimes be retrieved. In short, these systems should not be used to send or store anything they don't want others to read." This comment suggests that employees should not expect to have any privacy over workplace e-mail, irrespective of the provisions of the Privacy Act. This is in stark contrast to the approach of the Information Commissioner in the UK, who takes the view that employees do have privacy rights in relation to use of e-mail at work, as illustrated by the Draft Code of Practice (discussed in section 2.4.2 of chapter two). The Privacy Act can therefore be regarded as of somewhat limited use in protecting the rights of employees.

Having said this, in later reports the PCC shows some concern about e-mail and internet monitoring in the workplace. In his 1997-98 Annual Report, the PCC expresses some
dismay at the content of the Treasury Board’s new “Policy on the Use of Electronic Networks”, which includes monitoring powers. In particular, the PCC was concerned about, “a policy that might see federal employers assume a broad right to monitor the electronic activities of employees without specific justification.” The PCC had previously raised a number of points with Treasury Board staff when discussing an earlier draft of the policy, including the opinion that the policy should go no further than absolutely necessary to achieve the government’s legitimate goals as employer, and the recommendation that the least intrusive monitoring options should be used first. This approach appears to be using ideas of proportionality in placing limitations on employer monitoring, in a similar way to the Information Commissioner in the UK. The PCC criticises the Treasury Board for rejecting the suggestion that the least intrusive measures should be used first, and for seemingly considering e-mail to be inherently less private than telephone calls by allowing monitoring without consent. It should be noted however that the PCC does not allege that this policy is in breach of the Privacy Act, again illustrating the Act’s limitations. Instead, the PCC is using his wider powers to make more general (and unenforceable) recommendations about approaches towards privacy in the workplace, which are not actually required by law.

The Privacy Act is certainly directly relevant to the issue of e-mail and internet monitoring by government employers. The PCC also performs a valuable role, both in ensuring compliance with the Act, and in making wider recommendations about privacy-related matters which go further than the actual requirements of the Act. Such comments can influence the treatment of government employees, and possibly even employees who are not covered by the Act at all. However, the Act’s impact is limited in a couple of fundamental ways – it is only directly applicable to state employees, and the provisions of the Act itself provide only a certain degree of privacy protection.

277 Ibid.
279 Ibid. at 64.
280 Ibid. The PCC also notes that monitoring of telephone conversations in this way would be a criminal offence, presumably under the Criminal Code – although, as discussed above, these criminal law provisions appear to be of equal applicability to monitoring of e-mail and internet use.
3.1.3 The Personal Information Protection and Electronic Documents Act

The Personal Information Protection and Electronic Documents Act ("PIPEDA")\(^{281}\) was enacted by the Federal Government with the stated aim of recognising, "the right of privacy of individuals with respect to their personal information..."\(^ {282}\) The Act regulates the collection and use of "personal information", which is defined as any information about an "identifiable individual"\(^ {283}\). This definition seems to include personal information which is collected through monitoring of e-mail or internet use, and therefore the Act is directly relevant to the issues under discussion.

PIPEDA came into force on 1st January 2001 for federal undertakings, and will become applicable to all private organisations throughout Canada on 1st January 2004.\(^ {284}\) However, its scope is limited in relation to personal information about employees. The Act only applies to collection, use and disclosure of information in the course of "commercial activities".\(^ {285}\) Section 4(1)(b) provides that collection and use of information about employees is also covered by the Act, but only if this is done in connection with "the operation of a federal work undertaking or business." It therefore seems that employees of federal undertakings and businesses are protected by the Act, but other employees are not. The Act is therefore directly relevant to some employees, and is valuable in providing some general privacy principles, but fails to provide information privacy protection for employees within all types of business.

PIPEDA sets out privacy-protective principles which are very similar to those of the DPA in the UK.\(^ {286}\) These are contained in Schedule 1 of the Act, and a number are directly relevant to the issue of electronic monitoring by employers. Principle 2 specifies that the purposes for

\(^{281}\) SC 2000, c. 5.
\(^{282}\) Section 3.
\(^{283}\) Section 2(1).
\(^{284}\) Section 30. PIPEDA will not however necessarily apply to private undertakings in any province which has already enacted substantially similar legislation.
\(^{285}\) Section 4(1)(a).
\(^{286}\) Indeed, implementation of PIPEDA was at least in part due to the need for Canada to comply with the principles of the European Data Protection Directive (supra note 214), which requires member states to pass legislation prohibiting the transfer of personal data to countries which do not have adequate measures for data protection in place.
which information is being collected must be identified at or before the time of collection and should also be told to the individual in question, while Principle 5 specifies that information should not be used or disclosed for different purposes. This means that employees must be warned about monitoring practices in advance, and employers are limited to using collected information for previously identified purposes (as under the Privacy Act). However, PIPEDA also goes further, by including Principle 4, "Limiting Collection". This specifies that the collection of information should be limited to that necessary for the purposes identified by the organisation, and it is stated that, "Organisations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified." This introduces an additional restriction on employer monitoring practices which is missing from the Privacy Act, namely consideration of whether the practice in question is actually necessary in order to fulfil the employer's aims.

PIPEDA also contains requirements relating to consent, under Principle 3. This principle states that, "The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate." In order for consent to be "meaningful", it is stated that an individual must be able to reasonably understand how the information will be used or disclosed. In relation to electronic monitoring, employers will therefore need to be fairly specific about the way in which information will be collected and used, in order to obtain adequate consent from employees.287 However, it appears that consent can be implied – it is stated that organisations should generally seek express consent in relation to sensitive information, but implied consent would be appropriate for less sensitive information. "Sensitive" information is not defined, but it seems that implied

287 Advance knowledge and consent is not required where this is "inappropriate". Some examples are given of relevant circumstances – including legal, medical and security reasons, collection of information for the detection and prevention of fraud or for law enforcement, and where the individual is a minor, ill or incapacitated. These examples suggest that the exception should be interpreted fairly narrowly. Section 7 of the Act also contains some more specific exemptions to the consent requirement, section 7(1)(b) allowing collection of personal information where it is reasonable to expect that knowledge and consent would compromise the availability or accuracy of the information, and collection is reasonable for purposes related to breach of an agreement or contravention of law. This suggests that covert workplace monitoring could be carried out in order to detect breach of "agreed" workplace rules, as well as breach of the law, if the employer can show that otherwise the information's availability or accuracy would be jeopardised.
consent will be adequate in at least some circumstances. In the context of the workplace, this raises issues about the ability of employers to obtain implied "consent" by simply implementing workplace monitoring policies which are not objected to by employees.

However, the most significant provision of PIPEDA is the overriding principle contained in section 5(3). This provides that, "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." This sets a standard of "reasonableness" against which employer justifications of workplace monitoring practices will need to be tested — in effect, employers will have to justify both the scope of and rationale behind their monitoring policies. In contrast to the more limited approach of the Privacy Act, this introduces considerations of proportionality by looking at the specific circumstances of each case. As has been emphasised by the PCC in a recent speech, this means that consent alone is not enough — "Even if consent is being sought, the proposed invasion of privacy has to be appropriate under the circumstances." However, it appears that this test only applies to the purposes put forward by an employer, and does not require an assessment of the actual impact of the practice in question on individual privacy. If the purposes are judged to be appropriate, it seems that the practice can go ahead even if it is very invasive of privacy. There is no explicit requirement that the employer's and the individual's interests should be balanced against each other. Of course, it is not clear as yet how this provision will be interpreted in practice. On this interpretation, it does seem that the provision stops short of a full proportionality analysis. However, recent comments by the PCC suggest that PIPEDA could be more restrictive of employers. In the specific area of e-mail monitoring, the PCC has expressed the view that "the potential for problems does not justify wholesale monitoring", and even if there is a reason to suspect abuse of the system this can be addressed "in a less privacy invasive manner than monitoring everyone". The PCC is also sceptical about justifications of e-mail monitoring based on the need to avoid liability for harassment.

---

289 Supra note 72.
290 Ibid.
291 Ibid.
292 Ibid.
commenting that the requirement to exercise due diligence to prevent harassment “has never been interpreted as extending to wholesale monitoring of the workforce.”293 This approach towards e-mail monitoring suggests that the “reasonable person” standard could in fact be treated as a true proportionality test, whereby the invasiveness of the employer’s conduct will be considered as well as the reasons given for the conduct itself. If so, PIPEDA could potentially prove to be as significant in controlling employer practices as the DPA in the UK.

Overall, PIPEDA has introduced some substantive restrictions on employer monitoring practices. It appears that e-mail and internet monitoring can only take place for specific and open purposes, which will be judged against a “reasonableness” standard, and in most cases employees will need to have knowledge of and consent to the monitoring. However, as the Act only applies to employment in federal undertakings and businesses, it is also necessary to consider the privacy legislation enacted by various provinces.

3.1.4 Provincial Legislation

Five of the Canadian provinces have enacted specific privacy legislation – Saskatchewan, Newfoundland, Manitoba, British Columbia, and Quebec. Statutory protection of privacy is particularly well developed in Quebec, the only civil law jurisdiction in Canada. Although the Quebec experience is instructive about general approaches to privacy, this chapter will not consider the law in Quebec in any detail. The privacy laws in the common law provinces are more relevant to a comparative study with the United Kingdom, which takes a similar approach towards these issues. Civil law jurisdictions such as Quebec and European countries other than the UK (including France in particular) tend to have a somewhat different attitude towards privacy, generally adopting a much more privacy-protective stance. Although a study of such different legal approaches would be relevant to the present discussion, a detailed comparison with these jurisdictions is beyond the scope of this particular thesis and therefore will not be attempted here.294

293 Ibid.
294 Quebec provides protection for individual privacy in a number of ways. Firstly, a right to respect for private life in included in the Quebec Charter of Human Rights and Freedoms RSQ c. C-12 (which is
The remaining four provinces have all enacted legislation which creates a statutory tort of invasion of privacy. In Saskatchewan, Newfoundland and British Columbia, it is a tort "wilfully and without a claim of right" to violate individual privacy; in Manitoba, the tort is violation of privacy "substantially, unreasonably and without claim of right". In all of the provinces, monitoring and surveillance are expressly covered – both auditory and visual surveillance, and listening to or recording messages sent over a telecommunications system. It is therefore clear that potentially this tort is applicable to workplace monitoring, including interception of e-mail and monitoring of internet use.

The Saskatchewan, Newfoundland and British Columbia statutes all include a "balancing" test, which provides that the "nature and degree of privacy" to which an individual is entitled in any situation is that which is "reasonable in the circumstances, due regard being given to the lawful interests of others". This appears to be a proportionality test, whereby the impact of a privacy invasive practice must be weighed against other interests in light of the specific circumstances of the case. In relation to workplace monitoring, this means that the employer's reasons for carrying out the practice would have to be balanced against the effect on employee privacy. It is however somewhat unclear what would be seen as a "reasonable" degree of privacy in any given situation, and there appears to be wide scope for the courts to interpret this concept. Some guidance is provided as to when an act may be seen as invasive of privacy, namely taking into account the "nature, incidence and occasion" of the act, and "the relationship, whether domestic or other, between the parties". In the context of the workplace, the reference to the relationship between the parties does raise the possibility that

295 Saskatchewan (Privacy Act, RSS 1978 c. P-24); Newfoundland (Privacy Act, RSN 1990 c. P-22); Manitoba (Privacy Act, RSM 1987 c. P125); British Columbia (Privacy Act, RSBC 1979 c. 336).
296 Saskatchewan section 2; Newfoundland section 3(1); British Columbia section 1(1).
297 Manitoba section 2(1)
298 Saskatchewan section 3; Newfoundland section 4; Manitoba section 3; British Columbia section 4.
299 Saskatchewan section 6; Newfoundland section 3(2); British Columbia section 1(2).
300 Ibid.
an employment relationship might be regarded as significant. For example, the fact that the parties are in an employment relationship might mean that a workplace practice would not be seen as an invasion of privacy, even though the same conduct outside the workplace would be seen as impermissible -- this will depend on how much deference the courts are prepared to show towards employer interests in regulating the workplace.

In Saskatchewan, Newfoundland and Manitoba, the legislation also provides specific circumstances where conduct will not be an invasion of privacy. Two of these exceptions are potentially relevant to employer monitoring practices. Firstly, there will not be a violation of privacy if the individual has consented to the conduct, whether expressly or impliedly. Potential problems with the use of consent in this context are that of determining whether consent is truly voluntary, and the question of the scope of consent given in a particular context. Again, as discussed above in relation to PIPEDA, this raises questions about whether employees will be taken to have consented to privacy-invasive practices by simply acquiescing to a workplace monitoring policy. Secondly, there is an exception if the act or conduct was incidental to the exercise of a “lawful right”. In Saskatchewan and Newfoundland, this includes a right exercised in defence of “property”. This provision could be relied on by employers to justify monitoring of employees for a number of reasons. Defence of property could include e-mail and internet interception carried out in order to prevent theft or dissemination of confidential information, and on a wide interpretation might even include prevention of abuse of the employer’s equipment for private purposes during the employer’s time. In Manitoba, the exception goes further, and includes acts in defence of any “other interest” of the defendant. Potentially this could exempt any practice which is carried out by an employer in defence of its interests. Although the conduct must be reasonable and necessary for this purpose, this provision does provide a complete defence to a privacy claim irrespective of the severity of the impact on the claimant. The “balancing” test discussed above is not applied at all if the conduct in question falls under one of the

---

301 Saskatchewan section 4; Newfoundland section 5; Manitoba section 5.
exemptions.\textsuperscript{303} It can certainly be said that wide interpretation of these exemptions could reduce the effectiveness of the legislation.\textsuperscript{304} In contrast, British Columbia’s statute contains no specific exemptions, relying instead solely on the proportionality test.

Much of the uncertainty of the scope of this legislation can be seen as the result of deliberately broad drafting which would enable the laws to change with the times, and in 1980 it was commented that many decided cases were required to clarify the law.\textsuperscript{305} However, in practice the opposite appears to have happened. Perhaps surprisingly, this legislation has been relied on by employees in very few cases.\textsuperscript{306} Where it has been used, the couple of reported cases suggest that the provisions may in any event be interpreted in such a way as to favour the employer. In Saskatchewan, there has been one decision in which the Court showed considerable deference to the employer’s interests, \textit{UFCW Local 1400 \textendash; Saskatchewan Co-operative Association Limited (“UFCW Local 1400”).}\textsuperscript{307} This case concerned theft prevention measures by an employer which included covert video monitoring in the workplace. In relation to a claim under the Saskatchewan \textit{Privacy Act}, the Court found that there was no tort because the Act allowed privacy-invasive conduct which was in defence of property, and part of the employer’s function was to prevent activities which were causing losses to the business.\textsuperscript{308} A similar analysis could clearly be applied to a case of covert e-mail or internet monitoring. In British Columbia, the relevant Privacy Act was considered as part of a wrongful dismissal claim brought by an employee who was dismissed for sleeping on the job, in the case of \textit{Richardson \textendash; Davis Wire Industries Limited (“Richardson”).}\textsuperscript{309} The employee argued that covert videotape evidence of his misconduct

\textsuperscript{303} In contrast to the provisions of the HRA in the UK, where privacy-invasive practices are still subject to a proportionality test even if they are carried out for one of the potentially justified reasons listed in the Act.

\textsuperscript{304} Osborne (1980) \textit{supra} note 302 at 94.

\textsuperscript{305} \textit{Ibid.} at 110.

\textsuperscript{306} This could partly be due to the fact that these statutes have rarely been the subject of judicial interpretation at all, so giving judges and arbitrators little help in interpreting and applying them in the workplace context. See Bilsen (1992) \textit{supra} note 65 at 152. The legislation can be seen as having a number of problems which may deter individuals from making claims, including uncertain and unpredictable application, the fact that the plaintiff has the burden of proving the case, the existence of broad defences, and the fact that there is no access to the lower courts for small claims. See Osborne (1980) \textit{supra} note 302 at 108.


\textsuperscript{308} \textit{Ibid.} at 9.

\textsuperscript{309} (1997), 33 B.C.L.R. (3d) 224 (SC).
should not be admissible as it was obtained in violation of his right to privacy. The Court held that the videotape evidence was admissible. Kirkpatrick J expressed the view that the claimant had no privacy right in these circumstances because he "...could not reasonably expect to have the protection of privacy when he was sleeping on company time, on company property, and in circumstances where he could be expected to be contacted when needed."³¹⁰

Again, a similar analysis could be applied to an employee using company e-mail or internet facilities on company time. Kirkpatrick J also went on to find that even if the employee had a privacy right, the tape would still have been admissible because the Act merely provided the basis of a claim in tort and would not have prohibited admission of the evidence.³¹¹ Both of these decisions indicate that in practice the legislation may be of limited assistance to employees who believe that their privacy has been invaded at work.

Although these provincial statutes could potentially limit privacy-invasive monitoring practices by employers, it appears that they have rarely been relied on by employees. Where they have been used, employees have met with little success. It also appears that the defences which are provided in specific cases could also be interpreted fairly widely in the workplace context, exempting some or, in the case of Manitoba, all conduct carried out by employers in defence of their own interests. In summary, it can be said of the various Privacy Acts that "They have rarely been used, they have not been very successful, and they really do not address, successfully, the four privacy torts that Dean William Prosser identified..."³¹²

Although Ontario does not at present have any specific privacy legislation, consultation is currently taking place about a piece of new legislation which would make Ontario the second province (after Quebec) to enact a comprehensive privacy regime for the private sector. A consultation paper on a proposed Privacy Act has been issued by the Ministry of Consumer and Commercial Relations.³¹³ The proposals aim to protect personal information, and are

³¹² D. Flaherty, "Some Reflections on Privacy and Technology" (1999) 26 Man. L.J. 219 at 222. (For the torts referred to see Prosser (1960) *supra* note 6 and section 1.2.1 of chapter one).
based very closely on the provisions of PIPEDA. However, the legislation has a wider scope than PIPEDA – it will apply to private sector businesses, and is not limited to collection of information for “commercial” activities. This latter provision means that collection of information by employers for all types of purpose will be covered, and the paper specifically refers to internal use of information by employers as being included.\footnote{14}

The proposals include the same basic requirements as PIPEDA for the collection and use of personal information, namely collection for specific purposes with prior knowledge and consent of the individual. The same comments apply to these provisions as to PIPEDA, as discussed above. In relation to the consent requirement, the consultation paper states that, "Consent could cover a variety of future purposes and uses, as long as these have been clearly described beforehand."\footnote{15} This suggests that general advance consent to monitoring for a range of purposes would be permissible, such as could be obtained under an employment contract – although it appears that the employer would need to be fairly clear in specifying in advance the various purposes which might be covered. The proposals also contain an overall limitation on collection, use and disclosure of personal information, for "purposes a person would consider appropriate in the circumstances."\footnote{16} Again, as under PIPEDA, this appears to be a partial proportionality test, which does require scrutiny of the employer’s purposes but not necessarily consideration of the severity of the effect of the relevant practice on employee privacy.\footnote{17}

The proposals for an Ontario Privacy Act could place some significant limitations on the ability of employers to monitor e-mail and internet use by employees. The consultation paper also provides scope for sector codes to be developed to cover unique privacy needs, and specifically refers to codes for particular types of personal information “such as

\footnote{14} Ibid. at 3.
\footnote{15} Ibid. at 9.
\footnote{16} Ibid.
\footnote{17} The consultation paper does give one example of the application of this test, namely the fact that it would not be reasonable to collect racial or religious information where human rights legislation would prevent this information from being used to make a decision. It should be noted that this is a somewhat extreme example, where use of the information collected would actually contravene the law, and it is therefore unclear how limiting this provision will actually be on employer practices.
employee records". This suggests that the provisions of the Act could be made even more relevant specific issues of workplace privacy through development of sector codes, such as has been taking place in the UK through the Information Commissioner’s Draft Code. It appears that such codes would be developed by sector representatives, representatives of the public interest, and relevant experts, and would need to be approved by the Government. Although this stops short of empowering a regulatory body to make legally binding codes of practice, such as is the case with the Information Commissioner in the UK, there does appear to be scope for the Ontario Information and Privacy Commissioner (“the Ontario IPC”) to intervene and assist in developing a workplace specific sector code. This is particularly relevant as the Ontario IPC has already considered the issues of workplace privacy and use of e-mail systems.

In November 1993, the Ontario IPC produced a report on workplace privacy in general, including the issue of electronic monitoring of employees. The report recognised the impact which such practices could have on employees, and took the view that all employees have a right to a “privacy safety-net” which was not being provided by the existing law. The report recommended legislative action following consultation. It also set out three principles relating to electronic monitoring: covert surveillance should not take place without “extraordinary circumstances” and demonstrable cause for or suspicion of guilt; monitoring should be controlled through established rules about notification, purpose, and methods; and monitoring should be designed and used so that it does not collect information unrelated to work and work performance.

318 Supra note 313 at 16.
319 Supra note 211.
320 Supra note 313 at 16.
321 The Ontario Information and Privacy Commissioner’s mandate is to review government decisions and practices relating to information access and privacy, under the Freedom of Information and Protection of Privacy Act (RSO 1990 c. F-31) and the Municipal Freedom of Information and Protection of Privacy Act (RSO 1990 c. M-56). This role includes investigation of complaints, checking of compliance, educating the public, research and advice on access and privacy issues, and comment on proposed government legislation.
323 Ibid. at 12.
324 Ibid. at 13.
These principles were developed further in a specific report on e-mail systems, published in 1994. This sets out some general principles for use of e-mail, including the requirements that the privacy of e-mail users should be respected and protected, all organisations should have a specific policy on e-mail privacy, and e-mail systems should not be used for collecting, using and disclosing personal information without adequate privacy-protective safeguards. This report appears to take the view that employees can have an expectation of privacy over e-mails sent and received at work, and argues that “it is in the best interests of an organisation to offer the highest degree of privacy possible.” The question is one of when employer interests should be able to justify infringements of employee privacy. The principles set out in this report do appear to be limited in two respects. Firstly, it is stated that employees should not have an expectation of absolute privacy with respect to business information. This seems to fail to take account of the fact that a business communication may also reveal personal information about an employee. Secondly, the report emphasises that a policy should expressly inform employees about their rights and obligations regarding the use of e-mail, and comments that, “In the absence of a known corporate policy, most users of e-mail appear to assume that their communications are confidential.” Although not made clear, this does suggest that employers are able to limit the privacy of e-mails by defining employee expectations in a workplace policy. As discussed above in other contexts, this raises questions about whether employers should be able to define unilaterally an employee’s reasonable expectations of privacy at work. However, despite these caveats, it is encouraging that the Ontario IPC has already considered these issues on some detail, and will be in a position to contribute to the debate about the new Ontario Privacy Act with specific reference to employee privacy.

The federal and provincial legislation discussed above does have some impact on the issue of employer monitoring of e-mail and internet use by employees. However, the level of

326 Ibid. at 15.
327 Ibid. at 4.
328 Ibid. at 6.
329 Such as the example given by the UK Data Protection Commissioner in the Draft Code (supra note 211), where an employee discloses personal reasons for postponing a meeting in a business-related e-mail.
protection provided to employees varies widely depending on the province in which the employee is based, and whether the employment is federally or provincially regulated. There also appears to be little evidence that the existing legislation has been used by employees in this way. In any event, this legislation is all of general application, and is not directed towards the specific issues of either the workplace generally, or e-mail and internet monitoring in particular. In looking at how the Canadian law is dealing with the particular questions of electronic monitoring and privacy in the context of the employment relationship, it will therefore be helpful to turn to consideration of the relevant provisions of the Charter and application of privacy principles in grievance arbitrations.

3.2 Privacy and electronic monitoring under the Charter

The Charter does not contain any direct reference to a right of privacy. However, section 8 of the Charter provides a right to be secure against "unreasonable search or seizure". In the case of Hunter v. Southam, the Supreme Court confirmed that this provision should be interpreted in a purposive manner and protects an individual's "reasonable expectation" of privacy. In R v. Dyment, La Forest J described three "zones" or "realms" of privacy in the context of section 8 of the Charter, including information privacy which is clearly relevant to e-mail and internet monitoring.

It must be noted that the provisions of the Charter are of limited direct application to the workplace. Its provisions can only be relied on directly against the state (as is the case in the UK with the HRA), and therefore can be asserted directly only by state employees against their employer. However, principles developed under the Charter are also relevant to the development of the common law, and therefore may influence the outcome of disputes between private parties. Privacy principles developed under the Charter can thereby affect

---

330 Supra note 325 at 9.
332 Ibid. at 159.
333 Ibid. at 13.
334 Ibid. at 428. See also section 1.2.1 of chapter one.
335 See in particular RWDSU v. Dolphin Delivery, [1986] 2 S.C.R. 573, where the Supreme Court confirmed that the Charter could be asserted against the common law only if the state is involved, but
both public and private sector employees, and therefore these principles are very relevant to the present discussion about privacy in both the public and private workplace. The particular relevance of the Charter in grievance arbitration decisions is discussed further below.

Various decisions have elaborated on the circumstances in which an individual will have a “reasonable expectation” of privacy, with specific reference to the issue of electronic surveillance. In Hunter v. Southam, Dickson C.J. stated that the entitlement to a “reasonable expectation” of privacy indicated that, “...an assessment must be made as to whether in a particular situation the public’s interest in being left alone by the government must give way to the government’s interest in intruding on the individual’s privacy in order to advance its goals...”336 This appears to relate the question of whether an individual has an expectation of privacy to a proportionality test, whereby privacy interests are balanced against the government’s reasons for privacy-invasive conduct – describing the outcome of the balancing rather than defining the privacy interest in question.337 This leaves it somewhat unclear as to how the relevant privacy interest should be defined. It also contrasts with the approach towards reasonable expectations of privacy taken by the ECHR, where the concept is used to define whether a privacy interest is engaged at all, so that the proportionality test is only reached if the individual is found to have a reasonable expectation. However, subsequent cases concerned with electronic surveillance suggest that the correct approach is similar to that taken by the ECHR, and provide some guidance as to when such conduct will be regarded as infringing privacy.

In R v. Duarte,338 the Supreme Court considered the applicability of section 8 of the Charter to a case of covert audio-visual recording of a meeting between a police suspect, a police informant, and an undercover police officer. The Supreme Court held that participant surveillance (where one of the parties to a conversation has consented to the recording) is in breach of the Charter. La Forest J made it clear that “surreptitious” electronic surveillance was covered by section 8, and stated that, “one can scarcely imagine a state activity more

\[footnotesize
336 \textit{Supra} note 331 at 160.
337 L. Austin, "Privacy and the Question of Technology (on file with the author, 2001) at 19.
\]
dangerous to individual privacy than electronic surveillance."\textsuperscript{339} This was seen as very different from the risk that someone might repeat our words. In emphasising the particular dangers of electronic recordings, he stated that an unregulated power of electronic surveillance would, "annihilate any expectation that our communications will remain private", and would prevent an appropriate balance from being struck between the rights of the individual and the state.\textsuperscript{340} The question is put as one of striking a "fair balance between the right of the state to intrude on the private lives of its citizens and the right of those citizens to be left alone."\textsuperscript{341} This approach recognises the potential for electronic surveillance and monitoring to impact on individual privacy, and relies on a proportionality test in deciding whether an intrusion into individual privacy is justified. In all cases, this can only be done if the individual's right to privacy is outweighed.

However, in defining when an individual will have a "reasonable expectation" of privacy, La Forest J appears to rely on the question of whether the surveillance is surreptitious. In particular, he states that:

"...the assessment whether the surreptitious recording trenches on a reasonable expectation of privacy must turn on whether the person whose words were recorded spoke in circumstances in which it was reasonable for that person to expect that his or her words would only be heard by the persons he or she was addressing. As I see it, where persons have reasonable grounds to believe their communications are private communications in the sense defined above, the unauthorised surreptitious electronic recording of those communications cannot fail to be perceived as an intrusion on a reasonable expectation of privacy."\textsuperscript{342}

La Forest J goes on to comment that the \textit{Charter} must be taken to protect against recording of private communications "every time we speak in the expectation that our words will only be heard by the person or persons to whom we direct our remarks."\textsuperscript{343} This suggests that surveillance and monitoring will only infringe privacy if the individual is unaware of the practice. If the surveillance is overt, the individual will no longer have an "expectation" of

\textsuperscript{338} [1990] 1 S.C.R. 30.
\textsuperscript{339} \textit{Ibid.} at 43.
\textsuperscript{340} \textit{Ibid.} at 44.
\textsuperscript{341} \textit{Ibid.} at 49.
\textsuperscript{342} \textit{Ibid.} at 47.
\textsuperscript{343} \textit{Ibid.}
privacy and will be unprotected by the Charter. This is similar to the approach which appears to be suggested by the ECHR in the Halford case, whereby an individual’s right to privacy is defined by the extent to which the individual was led to believe that their communications were not being overheard.

These principles were developed further in the case of R v. Wong. This concerned video surveillance by the police of a hotel room which was being used for the purposes of illegal gambling. Again, it was found by the majority that the unauthorised surveillance was in breach of the reasonable expectation of privacy protected by the Charter. Delivering the majority judgement, La Forest J framed the question as one of whether the surveillance in question would diminish the privacy and freedom of citizens in a way which was inconsistent with the aims of a “free and open society”. In relation to surreptitious electronic surveillance, he stated that:

“...R v. Duarte makes it clear that to sanction such an intrusion would see our privacy diminished in just such an unacceptable manner. While there are societies in which persons have learned, to their cost, to expect that a microphone may be hidden in every wall, it is the hallmark of a society such as ours that its members hold to the belief that they are free to go about their daily business without running the risk that their words will be recorded at the sole discretion of agents of the state.”

Applying this to the present case, La Forest J confirmed that unauthorised video surveillance was also in breach of section 8 of the Charter. He also argued that this was very different from the risk that activities might simply be observed by others: “...the threat to privacy inherent in subjecting ourselves to the ordinary observations of others pales by comparison with the threat to privacy posed by allowing the state to make permanent electronic records of our words or activities.” This latter approach suggests that, in the context of the workplace, electronic monitoring can be seen as posing a greater threat to privacy than

---

345 Lamer C.J., in a dissenting judgement, argued that there was no reasonable expectation of privacy in a hotel room to which members of the public had been admitted. A reasonable person in these circumstances could expect that strangers, including the police, might be present in the room. (Ibid. at 63).
346 Ibid. at 46.
347 Ibid.
348 Ibid. at 48.
observation by supervisors and managers.

The majority judgement in this case bases the right to privacy on the values of a "free and open society". This suggests that a "reasonable expectation" of privacy is not based on an individual's expectations in particular circumstances, but more general expectations of what is appropriate in a free society. A practice could therefore be in breach of privacy rights even if the individual in question was aware that surveillance was being carried out – if the practice is nevertheless unreasonable, it breaches the privacy expectations of Canadian society. However, the extent of this principle is left somewhat unclear. Although expectations are expressly based on society's values, La Forest J's judgement also contains constant references to "surreptitious" or "clandestine" surveillance, and emphasises circumstances in which individuals do not expect to be watched or overheard. This suggests that the unexpected nature of the surveillance is still important, and it is not clear to what extent privacy is still protected if the individual is aware of the relevant conduct. He also contrasts Canadian society with the society of George Orwell's 1984, where "citizens had every reason to expect that their every movement was subject to electronic video surveillance." This analogy could be seen as confirmation that privacy rights can still apply even where individuals are expecting to be watched. However, it could also be seen as a contrasting case where there is no expectation of privacy. If so, would a workplace in which all employees expected to be monitored at all times succeed in obliterating employee privacy rights? Presumably the values of a free society could still be applied so as to provide protection. However, the judgement in Wong does appear to leave open the issue of whether surveillance must be covert in order to be in breach of reasonable expectations of privacy. Overall, the choice can be summarised as being between an empirical conception of the definition of privacy interests, whereby privacy expectations depend on the factual circumstances and what an individual has actually been led to believe, and a normative

---

349 See Austin (2001) supra note 337 at 22.
350 Supra note 344 at 47.
351 See Austin (2001) supra note 337 at 23-24, who argues that this example shows a change of emphasis from whether individuals expect their activities to be watched, to a question of whether something is a reasonable practice even if it is expected.
conception whereby expectations are based on external values. As will be discussed further in section 4.2.1 of chapter four, in the context of the employment relationship, approaches based on a purely empirical definition of reasonable expectations provide inadequate protection of employee privacy, because this gives the employer too much power to define unilaterally an employee’s privacy expectations.

These cases show clearly that privacy rights under the Charter do apply to cases of electronic monitoring, which by analogy would include e-mail and internet interceptions. However, the precise scope of an individual’s “reasonable expectation of privacy” still remains somewhat unclear, and none of these decisions apply the principles to the employment relationship. A direct action for breach of privacy under the Charter can also only be brought by public sector employees. It will therefore be helpful to look at how general privacy principles drawn from the Charter (and elsewhere) have been applied to private sector workplace disputes in both the common law and grievance arbitration decisions.

3.3 Privacy in employment law

In Canada, the common law relating to the employment relationship is based on the concept of the individual contract of employment (and is generally termed “employment law” as opposed to “labour law” which deals with unionised employees). The common law implies an entitlement to “reasonable notice” of dismissal into each employment contract, and failure to give such notice results in a wrongful dismissal claim. It appears that, to date, the right to privacy has not been considered in any reported wrongful dismissal cases. However, in theory privacy could potentially be relevant to wrongful dismissal claims in two ways – in judging the fairness of the employer’s conduct, and in deciding questions of admissibility of evidence.

See Austin, ibid., at 27, who classifies the distinction as the difference between a “conventional norm” approach (whether a reasonable person would expect privacy), and an “independent justification” approach (based on the independent values underlying the protection of privacy). This treats both tests as objective, but adopts the same underlying analysis as the empirical/normative distinction set out above - distinguishing between an approach whereby surreptitious monitoring is wrong because it defeats conventional privacy expectations, and an approach whereby any type of monitoring can be wrong if it violates the values underlying privacy irrespective of factual expectations.
The question of whether an employer owes an implied obligation of fairness towards employees at common law has not yet been settled by the courts. However, if such considerations can be relevant to a wrongful dismissal claim, then there is scope for a tort of invasion of privacy in the workplace to be developed. Prying into employees’ private lives, including by such means as video, e-mail and internet monitoring, could certainly be seen as bad faith conduct. However, it seems that this argument has yet to be considered.

Another common-law based argument that has not yet been developed relates to admissibility of evidence – specifically, a situation where evidence of wrongdoing relied on in dismissing an employee has been obtained in an impermissible manner. Again, privacy considerations could be relevant here. Courts could certainly adopt the practice of excluding evidence obtained in breach of an employee’s privacy rights, such as can happen in arbitrations in relation to video surveillance evidence, and similarly by analogy evidence obtained through privacy-invasive computer monitoring.

The lack of examples of application of a right of privacy in common law employment cases is perhaps a reflection of the fact that a general common law tort of invasion of privacy has not yet been fully developed by the Canadian courts. There are a few cases in which the existence of such a tort has been suggested, including some decisions of lower courts in Ontario, and it has been argued that there is scope for a common law tort to be developed on the basis of Charter values. However, a general common law privacy right has not yet been established, and consequently such a right has not been applied in the workplace context. It remains somewhat surprising that this argument has not yet been developed, in light of the increasing prevalence of potentially privacy-invasive workplace practices. It is

353 In the case of Wallace v United Grain Growers (1997), 152 D.L.R (4th) 1, the Supreme Court of Canada denied the existence of an independent tort of “bad faith” discharge, but in extending the employee’s reasonable notice period did go on to rely on the unfair way in which the employee in question had been dismissed.
355 Ibid.
356 Ibid. at 10.28 footnote 4.
certainly possible that a right of privacy could be used in wrongful dismissal cases in the future, depending on how the general law evolves. However, in light of the lack of current examples, consideration of the common law is of little present assistance in analysing workplace privacy issues. It is therefore more helpful to turn to grievance arbitration jurisprudence, where there has been greater willingness to rely on privacy considerations in deciding workplace disputes.

3.4 Privacy and electronic monitoring in grievance arbitrations

In Canada, employees in a unionised workplace are unable to bring an action against their employer for wrongful dismissal. Such employees have their workplace terms and conditions governed by a collective agreement, and where such an agreement is in force legislation requires that all disputes over terms and conditions are referred to compulsory binding arbitration. Labour arbitration is an adjudicative process which focuses on interpretation and application of the terms of the collective agreement. All collective agreements contain provisions against dismissal without just cause, and empower the arbitrator to award reinstatement as well as damages. The process of grievance arbitration can be distinguished from that of interest arbitration, a method of dispute resolution where the arbitrator actually makes binding terms and conditions of employment.

As will be discussed further below, arbitrators have been prepared to consider issues of workplace privacy in a number of different contexts, and arbitral jurisprudence is therefore a useful source of privacy principles in Canada. However, there are some limitations on the extent to which privacy considerations can be brought into arbitrations, in light of the fact that the process is based upon interpretation of the contractually binding terms of a collective agreement. Application of the general law in arbitrations is required, and arbitrators may also be given power to draw on employment-related statutes in making their decision.\(^\text{359}\)


\(^{359}\) See for example section 48(12)(j) of the *Ontario Labour Relations Act* SO 1995 c.1 Sch A, which provides that an arbitrator or arbitration board has the power “to interpret and apply human rights and
However, the basic principle is that arbitrators are largely confined by the scope of the contract negotiated between the parties. This would suggest that, where the terms of a collective agreement are clear and do not appear to disallow a privacy-invasive practice, an arbitrator has limited power to intervene in order to uphold employee privacy. Arbitrators have nevertheless developed a number of ways in which workplace privacy can be protected.

Grievance arbitrations may arise from an individual grievance about application of the collective agreement, often related to discipline or dismissal, or a more general challenge to an employer's workplace practices. In relation to individual discipline, privacy principles are most often considered by arbitrators in deciding whether or not to admit evidence of wrongdoing gathered by the employer in a privacy-invasive manner, for example through searches or covert surveillance. In the context of union challenges to workplace policies, introduction of privacy-invasive practices may actually be in breach of an express clause of the collective agreement. Although it is relatively rare for the collective agreement to deal directly with these issues, it can potentially happen in two ways\(^{361}\) - there could be a clause which expressly protects the right of privacy in the workplace, or alternatively a clause which restricts the employer's practices by other means, such as one guaranteeing the maintenance of working conditions.\(^{361}\) Privacy considerations may also be relevant to interpretation of a management rights clause in a collective agreement. Traditionally, management has been seen as free to act as it sees fit, subject to any express limitations in the collective agreement, and the duty to act in good faith and not jeopardise the integrity of the bargaining unit.\(^{362}\) However, a management rights clause may contain an express requirement that managerial discretion be exercised reasonably and/or fairly, in which case privacy considerations may be relevant in assessing the reasonableness of the employer's conduct. Even if the collective agreement is silent on this issue, some arbitrators have been prepared to imply into the collective agreement the principle that employers must act fairly and reasonably in exercising management prerogatives. This would again give arbitrators scope to challenge the

---

361 See for example Re Thibodeau-Finch Express Inc and Teamsters Union, Local 880 (1988), 32 L.A.C. (3d) 271 (Burkett, Ontario) (discussed further below).
implementation of privacy-invasive practices by employers. Although rare nowadays, some arbitrators have refused to acknowledge the existence of a general principle of fairness.\(^{363}\) The express wording of a collective agreement must also be given effect to, and therefore a clear management rights clause together with a clause preventing an arbitrator from adding to or amending the agreement would prevent the employer from being under an obligation to act fairly. This means that the position relating to management's duty to act fairly and reasonably remains somewhat unsettled.\(^{364}\)

The issue of interpretation of collective agreements in light of general privacy principles links to the question of whether arbitrators can take account of Charter principles in grievance arbitrations. Even prior to the implementation of the Charter in 1982, arbitrators had begun to rely on general principles which afforded protection to employee privacy, in particular in relation to searches of employees.\(^{365}\) With application of the Charter, it appears that two schools of thought have developed - a cautious approach based on the analysis that the Charter is designed to protect against abuse of power by the State and is not applicable between private parties, and a broader view that the fundamental rights and freedoms contained in the Charter should be applied in interpreting the law and deciding disputes.\(^{366}\)

An example of the broader approach in the context of workplace privacy is the case of Re Domon Forest Products Ltd and IWA Local 1-357,\(^{367}\) which concerned the admissibility of covert video surveillance of an employee who was away from work on the grounds of ill health. Arbitrator Vickers took the view that collective agreements should be interpreted in light of the fundamental values under the Charter, including the right of privacy. In deciding the case in accordance with the principles underlying section 8 of the Charter, he went on to adopt the "reasonableness" test set out by the Supreme Court in Hunter v-
Although this approach towards use of Charter values in grievance arbitrations is not universally accepted, it does provide additional scope for privacy considerations to be brought into workplace disputes, particularly in relation to interpretation of the managerial duty to act fairly and reasonably. However, it should be noted that even if arbitrators are prepared to look to Charter values in interpreting collective agreements, it appears that an express clause in such an agreement will still enable the employer and the union to "contract out" of the right to privacy.

Bearing these general principles in mind, one can turn to the question of how arbitrators have addressed the specific issue of workplace privacy in relation to e-mail and internet monitoring, and the analogous issue of workplace video surveillance.

3.4.1 Monitoring use of e-mail and computers in the workplace

There are very few arbitration decisions which consider specifically the employee’s right of privacy over e-mails and other use of computers at work. It is perhaps somewhat surprising that there are not more decisions in this area. It is not uncommon for grievances to be based on the dismissal of an employee for abuse of e-mail or internet facilities, but it appears that to date unions have rarely argued the employee’s right to privacy as part of such a claim.
Those arbitrators who have considered the issue have taken a somewhat limited view of employee privacy, but it is worth considering the decisions in some detail in order to discover which principles seem to be being applied.

A search of computer files by an employer was considered by Arbitrator Bruce in *International Association of Bridge, Local Union No 97, and Structural and Ornamental Ironworkers, and Office and Technical Employees' Union, Local 15* ("International Association of Bridge"). The grievor in this case complained that a decision to suspend her for performing personal projects during working hours was based on evidence gathered in breach of her right to privacy. In particular, the employer had searched and recovered files which had been deleted from the hard drive on the grievor’s workplace computer, some of which had been protected with a personal password. Arbitrator Bruce noted that breach of privacy in general and the rights and freedoms guaranteed by the Charter were relevant to the concept of a fair hearing, and addressed the issues of whether the grievor had a reasonable expectation of privacy over personal work on the computer, and whether the employer had reasonable grounds for searching the files. He found that the grievor’s privacy had not been violated, and the search had been carried out on reasonable grounds.

In considering the issue of the grievor’s reasonable expectation of privacy, Bruce looked at a number of factors. These included the fact that the computer equipment in question belonged to the employer, the fact that the employer had not searched private property or carried out clandestine monitoring of conduct, and the fact that the grievor had been instructed not to perform personal work during the employer’s time. Bruce also relied specifically on the fact that all documents typed on the grievor’s computer were copied into the employer’s mainframe and could be accessed through the computer network, and the grievor was aware that her files could be accessed in this way. This last factor seemed to be particularly relevant to the finding that employees in this workplace did not have a “reasonable expectation” that workplace computer files would remain private. This indicates that an

---

373 Although it is not clear how a clandestine search of an employee’s computer files is qualitatively different from clandestine monitoring of conduct through electronic means.
374 Supra note 372 at paragraph 64.
employer is able to define an employee's expectations of privacy at work. In the same way as is suggested by the decision of the ECHR in the Halford case, and some aspects of the Supreme Court decisions concerning section 8 of the Charter referred to above, it is the employee's actual expectations which are important – if the employer has led the employee to believe that they have no privacy over communications, then the employee is unable to assert privacy rights. The grievor knew that the employer could in theory access the files, and therefore the employer had a right to do so. This is despite the fact that the grievor in this case had taken the step of protecting some of the files with a computer password in order to try and keep the material private, which the employer had to break in order to access the information. 376

Arbitrator Bruce does go on to consider whether the employer had reasonable grounds for the search. This seems to involve a proportionality analysis, whereby the employer's need to gather evidence in this way is tested. He relies on the grievor's past history of personal work during working hours, previous letter of reprimand, suspicious behaviour, and the fact that the employer had no reasonable alternative means of obtaining evidence, in finding that the search was reasonable. 377 This test of the "reasonableness" of the employer's behaviour would seem to provide additional protection for the employee's privacy. However, it appears that this analysis is not actually necessary if the employee does not have a reasonable expectation of privacy in the first place.

The only reported decision to deal directly with the issue of employer e-mail monitoring is that of Arbitrator Germaine in Camosun College -v- Canadian Union of Public Employees, Local 2081. ("Camosun College") 378 This decision is not protective of employee privacy. The case concerned the dismissal of an employee for sending a lengthy and inappropriate e-mail message to a union "chat group" on the employer's computer network, which was forwarded to the employer by another subscriber to the group. Arbitrator Germaine

375 Ibid.
376 In contrast, the Draft Code issued by the Information Commissioner in the UK suggests that material clearly intended to be private on a workplace computer should not be accessed by the employer (supra note 211 and see discussion in section 2.4.2 of chapter two).
377 Supra note 372 at paragraph 65.
considered a variety of factors in deciding that the circumstances did not involve the grievor’s right to privacy. He emphasised that the message should not have been regarded as confidential. Not only was the e-mail list part of the employer’s system, but any of the subscribers to the list could print or forward the messages, and the union did not extend any assurances of confidentiality to subscribers. Again, this is taking an approach towards reasonable expectations of privacy which relies on whether the individual had been led to believe that communications would not be intercepted. The union and the grievor “appreciated the relevant characteristics of electronic mail”, and therefore could not claim confidentiality.

Arbitrator Germaine also relied on two previous decisions, Smyth v. Pillsbury Corporation, a decision from the United States District Court for the Eastern State of Pennsylvania, and the unreported arbitration decision of Arbitrator Weiler in Insurance Corporation of British Columbia. Both of these cases decided that there was no reasonable expectation of privacy in e-mail communications. In the previous arbitration decision, Weiler found that communications by e-mail were different from private letter mail or telephone conversations, and did not involve the same expectation of privacy. The rationale for this approach is unclear, but appears to be based on the fact that the employee is using the employer’s property – although the same argument would seem to apply to use of the employer’s telephone system. In Smyth v. Pillsbury, the employer had actually given assurances to employees that e-mails would not be intercepted, but nevertheless an interception by management was found not to be an invasion of privacy. The Camosun College decision therefore goes further than simply establishing that there is no expectation of privacy if employees know that e-mails may be intercepted. The two previous decisions relied on seem to indicate that employees simply do not have any expectation of privacy over workplace e-mail, which by its very nature is never regarded as private in any circumstances.

---

379 Ibid. at paragraphs 22-23.
380 Ibid. at paragraph 24.
381 It should be noted that the publication of an e-mail by sending it to a chat group could be regarded as very different from the sending of a private message from one individual to another. It could be argued that these circumstances did not involve a private interest at all, particularly as the chat group was not confidential. However, the case itself was decided on more generally on the basis of the characteristics of electronic mail, and is therefore a useful example of attitudes towards e-mail privacy.
382 914 F Supp 97 (E.D.Pa. 1996)
This means that employers apparently have a free hand to intercept e-mails as they see fit.

Despite the restrictive approach of the Camosun College decision, it is still possible that future decisions in this area will be more protective of employee privacy. As is discussed further below, arbitrators could extend privacy principles developed in relation to workplace video surveillance to situations of e-mail and internet monitoring. It is also worth considering whether the decision in Smyth v. Pillsbury is actually an appropriate one to be relied on by Canadian arbitrators.

*Smyth v. Pillsbury* concerned the dismissal of an employee for sending inappropriate comments over the employer’s e-mail system. The employer intercepted and relied on these e-mails, despite the fact that it had assured all employees that e-mail communications were regarded as confidential and would not be intercepted. As Pennsylvania is an employment-at-will jurisdiction, the employee’s claim was based on the fact that his dismissal in breach of his right to privacy (a tort in Pennsylvanian law) violated a “clear mandate of public policy”, an exception to the employment at will rule which was noted by the Court to be a particularly narrow one. Under Pennsylvanian law, the tort of privacy is only made out if an intrusion is “substantial and would be highly offensive to the ‘ordinary reasonable’ person.” In light of the restrictive nature of this test, it is perhaps unsurprising that the employee’s claim was not successful. Certainly this is very different from the general considerations of reasonableness which would be applied in a Canadian grievance arbitration, and a different standard to that applied under the various Canadian provincial statutory torts and other privacy legislation. The Court noted that the employer was not requiring the employee to disclose personal information about himself, and the employer’s interest in preventing inappropriate comments and illegal activity outweighed any privacy interest; however, the analysis might have been different if the test had not been one of whether the invasion of privacy was “substantial and highly offensive”.

---

384 Supra note 382 at 99.
385 Ibid. at 100.
Perhaps more problematic is the Court’s prior finding that the employee did not in any event have any expectation of privacy over e-mail communications. The Court took the view that the employee lost any “reasonable expectation of privacy” in the communication as soon as it was sent over an e-mail system used by the entire company. It is not explained in the decision why the simple fact that the e-mail was sent over the company’s system resulted in a loss of privacy, or why the assurances previously given by the employer did not make a difference. It appears that the Court misinterpreted the nature of e-mails sent over a company network, treating them like messages broadcast to all users of the system rather than messages sent specifically from one point to another.388 This unusually restrictive treatment of workplace e-mail appears to be based on flawed assumptions, and it is therefore questionable whether the view of reasonable expectations of privacy taken in the case should be followed in future decisions.389 In light of the problems with Smyth v. Pillsbury, this cannot be regarded as an appropriate precedent for the development of Canadian law in this area.

3.4.2 Monitoring through workplace video surveillance

Although there is presently a shortage of arbitration decisions dealing with the issue of e-mail and internet monitoring in the workplace, there is already a considerable body of jurisprudence concerning other invasions of employee privacy. The issues considered include physical searches and searches of personal effects, drug testing, and electronic video surveillance both outside and within the workplace. It is entirely possible that the principles developed in these cases will be extended to invasions of privacy through e-mail and internet.

387 Supra note 382 at 101.
388 Morgan (1999) supra note 55 at 871. See also R. Dixon, “Windows Nine-to-Five: Smyth v. Pillsbury and the scope of an Employee’s Right of Privacy in Employer Communications” (1997) 2 Va. J. L. and Tech. 4, who argues that the decision is flawed for a number of reasons: it misunderstands the nature of the relevant technology, is inconsistent with cases about telephone monitoring (particularly as increasingly voicemail and e-mail may be provided over the same system), it is particularly unhelpful as developments in internet technology are blurring the line between activities carried out over the employer’s network and purely external communications, and appears to confuse the notion of privacy with that of solitude.

389 It should be noted that some previous decisions from California has already considered the issue of employees’ expectations of privacy over workplace e-mail. These had also taken a restrictive approach, although they did not go so far as a general principle that workplace e-mails could never be regarded as private. See in particular Flanagan v. Epson, Cal Super Ct, Los Angeles County, 1990, Docket No BC 007036 (no expectation of privacy over business-related communications), and Bourke
monitoring. The issue of video surveillance of employees within the workplace seems to provide a particularly appropriate analogy, and raises a number of questions which apply equally to e-mail and internet surveillance. Both practices primarily infringe on informational privacy. Video monitoring may be covert, but the employer may also be open about the practice, and may even implement a workplace policy accordingly. The reasons why employers may want to monitor employees are also very similar, including prevention of theft, deterrence of inappropriate behaviour, and performance assessment. As with e-mail and internet monitoring, video surveillance for business related reasons may nevertheless pick up private conduct or information as well. Video monitoring within the workplace (as opposed to surveillance of off-duty behaviour by employees) also raises similar issues about the extent to which employers are able to control working methods and equipment, and run the workplace as they see fit. Analysis of some of the jurisprudence about workplace video surveillance may therefore be particularly instructive in considering how employee privacy rights over e-mail and internet use may be developed.

A number of arbitration decisions have expressly considered the general scope of an employee’s right to privacy in the specific context of workplace video surveillance. One of the earliest cases to deal with this issue was Puretex Knitting Co Ltd and Canadian Textile and Chemical Union ("Puretex"). This was an interest arbitration concerning video cameras which had openly been installed by the employer in the workplace for the purposes of deterring theft, although without consulting with the relevant union in advance. Arbitrator Ellis ordered the removal of cameras which had been placed in the production areas of the factory. In categorising the rights at stake, Ellis recognised that the issue of electronic surveillance involved “conflicting social values of considerable significance”, namely the rights to privacy and human dignity, as balanced against considerations of efficiency. He expressed the view that the issues are the same in the industrial context, and went on to set out the relevant test as follows:

---

390 See section 1.5 of chapter one for a full discussion of reasons for employer monitoring, nearly all of which could equally apply to video surveillance.

391 (1979), 23 L.A.C. (2d) 14 (Ellis, Ontario).

392 Ibid. at 29.
"It is clearly a matter of balancing competing considerations after recognising that any use of cameras that observe employees at work is intrinsically seriously objectionable in human terms, with the degree of objection depending on the way the cameras are deployed and the purpose for which they are used and ranging from unacceptable in the case of constant surveillance of conduct and work performance to probably non-objectionable in the case of short-term individual application for training purposes."393

The approach is clearly one of proportionality – the competing interests of employer and employee must be balanced against each other, taking into account the severity of the effect on employee privacy and the reasons for the surveillance, together with the way in which it has been carried out. It is interesting that there is no consideration of the employee’s “reasonable expectation” of privacy. This was a case of overt surveillance, where the employees were fully aware of the practice. Under the analysis adopted in the arbitrations discussed above concerning use of computers and e-mail, and arguably under the Supreme Court analysis in the Charter privacy cases, this fact would have defeated the employees’ claim – they knew about the monitoring, and therefore had no expectation of privacy. In contrast, this factor is entirely unimportant to Ellis. The employees’ interests are categorised as involving human dignity, and therefore can be infringed whether or not the surveillance in question is surreptitious.

This approach towards employee privacy has been followed by arbitrators in a number of subsequent cases. In Re Thibodeau-Finch Express Inc and Teamsters Union, Local 880 ("Thibodeau-Finch"),394 the majority of the arbitration panel endorsed the analysis in Puretex in the context of overt video surveillance in the maintenance area of the employer’s premises. The panel recognised that the issue was one of a conflict between the employee’s privacy rights and the employer’s right to maintain the security of his business, and although they expressed the view that a search of an individual’s person or belongings was a greater intrusion on privacy than general surveillance, they also had the same "instinctive concern

393 Ibid. at 30.
394 Supra note 361.
about camera surveillance of the workplace” as was articulated in Puretex.395

This analysis of surveillance and privacy was developed further by Arbitrator Larson in St Mary’s Hospital (New Westminster) and Hospital Employees Union (“St Mary’s”).396 This was a case of covert video surveillance of employees in a particular work area, and Larson applied principles drawn from the British Columbia Privacy Act in making a binding recommendation that the use of cameras in this way was inappropriate in the circumstances. The decision approves the comments in Thibodeau-Finch, and also refers in some detail to the test of balancing of interests used in cases of surveillance of employees outside the workplace.397 It goes on to set out a hierarchy of protections afforded by the right to privacy.398 Most protected are bodily intrusions by an employer, followed by searches of personal effects and spaces. Surveillance cases are seen as analogous to searches of personal effects, but the extent of right to privacy depends on the type of surveillance – benign surveillance for the benefit of employees (such as for training purposes) will require little justification; surveillance for the purposes of security comes next, and it is noted that this often takes place openly and with the implied consent of the union; finally, surreptitious surveillance will require the most justification.399 This appears to revert to some extent to the idea of reasonable expectations of privacy. Although it is recognised that open surveillance can in principle infringe privacy, covert surveillance is seen as the practice which is most offensive to privacy rights - somewhat different from the emphasis in Puretex on the affront which surveillance poses to human dignity irrespective of the employees’ state of knowledge. Finally, Larson sets out the considerations which must be taken into account in balancing the relevant interests. The employer must demonstrate cause to initiate the surveillance, act in conformity with the collective agreement, show that it has exhausted all less intrusive alternatives, and ensure that the surveillance is systematic and non-discriminatory.400 In applying this proportionality test, Larson found that the employer had failed to minimise the

395 Ibid. at 281. It should however be noted that the result in this case, a direction that the cameras should be removed, was not itself based on privacy arguments but on interpretation of express terms of the collective agreement (discussed further below).
397 Ibid. at 391 to 395.
398 Ibid. at 397 to 398.
399 Ibid. at 398 to 399.
400 Ibid. at 399.
intrusions on employee privacy, noting that:

"...the right to privacy is a basic human right which must be not only guarded but which must also be nurtured through mutual respect and understanding. The privacy of a group of employees is so important that an employer must do everything reasonably possible to secure its property before it is entitled to initiate clandestine surveillance."401

A final example of arbitration decisions which expressly recognise employee privacy is the case of \textit{Re Brewers Retail Inc and United Brewers' Warehousing Workers' Provincial Board ("Re Brewers Retail").}402 This involved covert surveillance of an individual employee based on suspicion of drinking, fraud and theft. Arbitrator Herman ultimately found that in the specific circumstances of the case the decision to videotape the grievor in both the company's warehouse and retail lobby was reasonable.403 However, this was only after full consideration of the privacy issues, and both parties in the case accepted that in Ontario arbitrations employees have a right of privacy which is balanced against the employer's right to manage the workplace. After a review of the caselaw, Herman adopted a two stage proportionality test: "whether it was reasonable in the circumstances for the company to have resorted to surreptitious videotaping, and if so, whether the videotaping itself was carried out in a reasonable manner."404 The decision goes on to consider more general issues about employee expectations of privacy in the workplace. In particular, the employer's argument that employees did not have a reasonable expectation of privacy when working was expressly rejected. Herman makes it clear that covert video surveillance can be an "affront to human dignity" wherever it takes place, stating that: "The rationale for imposing restrictions, and for balancing the interests of the employer and the individual employee, remains the same whether the videotaping takes place while the employee is in the workplace, working elsewhere, or off duty. It is the employee's right to be protected from invasive covert

\begin{footnotes}
401 \textit{Ibid.} at 400.
402 \textit{(1999), 78 L.A.C. (4th) 394 (Herman, Ontario).}
403 This was based on the fact that videotaping in the retail lobby was the only realistic way to determine whether the grievor was drinking at work, in light of the fact that this was in any event a public space and so the grievor had limited privacy, and the videotaping in the warehouse was a last resort after other efforts to deal with the grievor's drinking problem had failed (\textit{Ibid.} at 425-428).
404 \textit{Ibid.} at 417.
\end{footnotes}
videotaping that is at issue, whatever the venue.\footnote{405} However, as in St Mary's, there is a suggestion in the decision that an employee's expectations of privacy may depend on his or her awareness of the surveillance. Herman comments that the grievor's expectations of privacy would differ depending on whether the surveillance was in the lobby, where he was aware of the presence of a CCTV camera and also could be seen by members of the public, as compared to surveillance in the warehouse where he was not aware of any videotaping or ongoing scrutiny.\footnote{406} Again, this suggests that employers can limit exposure by being open about surveillance practices; although this might still infringe privacy (rather than defeating privacy expectations altogether), employers may require a less compelling justification for such conduct than where surreptitious surveillance is involved.

These grievance arbitration decisions provide more comprehensive protection of employee privacy than any of the other caselaw or legislation discussed so far, effectively requiring a balancing of the employer's and the employee's interests in all cases. However, there are a number of limitations on the scope of these decisions which need to be considered. There are reasons why the principles applied in these cases might not be applicable to all types of grievance arbitration. There are also some conflicting decisions. These other decisions not only show a reliance on the strict wording of the relevant collective agreement, but also question the more fundamental principles about whether other laws such as the Charter is relevant to arbitrations, and whether privacy in the workplace has equal force to privacy elsewhere.

As outlined above, arbitrations can take place in a variety of circumstances. Only one of the discussed four cases actually involved a challenge to a management practice under the terms of a collective agreement. Therefore they do not shed much light on the difficult issue of whether arbitrators can limit management rights under the terms of a collective agreement, which appears to allow privacy invasive conduct. Puretex was an interest arbitration, where the arbitrator was asked to make a binding ruling about the practice of surveillance in order to resolve a dispute. Similarly, in St Mary's the arbitrator had been asked to make a binding
recommendation. This case also relied on principles drawn from the provincial *Privacy Act*, which would not be applicable in provinces without such legislation. *Re Brewer’s Retail* concerned the reasonableness of an individual dismissal and the admissibility of evidence obtained through surveillance. Although *Thibodeau-Finch* did deal with a union grievance under a collective agreement, it should be noted that the comments about privacy principles outlined above were actually *obiter* – the case itself was decided on the basis of the precise wording of the collective agreement, namely breach by the employer of a clause about maintenance of operational practices. Arbitrators who have been confronted with a challenge to surveillance practices under a collective agreement have seemingly found it more difficult to uphold privacy rights in the face of clear contractual wording, particularly in Ontario which presently lacks general privacy legislation.

For example, in the case of *Re QBD Cooling Systems Inc and Canadian Union of Operating Engineers and General Workers, Local 101* (“*Re QBD Cooling Systems*”), the union challenged the employer’s decision to install video monitoring equipment throughout the plant for the purposes of deterring theft. Arbitrator Newman found that the grievance was not arbitrable at all, relying entirely on the strict wording of the collective agreement. She found that there could be no requirement of “reasonableness” implied into the exercise of management rights under the agreement, because in accordance with the agreement’s wording, any such limitations would require an express provision. The intention of the parties was clear, there was no such express limitation, and therefore the employer had the right to implement surveillance in accordance with its general powers under the management rights clause. There is no consideration in the decision of general principles of employee privacy at all (although it does not appear that this was in any event actually argued by the union).

Two subsequent Ontario grievance arbitrations take an even more restrictive approach towards protection of employee privacy in the workplace. In *Re Lenworth Metal Products Ltd and United Steelworkers of America, Local 3950* (“*Re Lenworth*”), the issue was

---

again a challenge to the installation of security cameras under the terms of a collective agreement. Arbitrator Armstrong took the view that the cases about surveillance of employees outside work were of limited assistance, as they raised "...quite a distinct issue from the manner in which an employer organises and operates its workplace, either to protect the security of its premises and property or to scrutinise the conduct, behaviour and performance of employees at work, or for other miscellaneous purposes." In contrast to the approach in Puretex and Re Brewers Retail, which treat the issue as one of "human dignity" irrespective of whether the surveillance is carried out during or outside work, Armstrong adopts a deferential approach towards the employer's right to organise and run its own workplace. The decision goes on to distinguish some of the previous arbitration decisions, noting in particular that Puretex was an interest arbitration, the comments in Re Thibodeau-Finch about privacy were not the ratio of the decision, and Re St Mary's applied the British Columbia privacy legislation. Armstrong takes the view that, in Ontario, there is no Privacy Act and therefore no legal principle that surveillance is an invasion of any privacy right. He also rejects the argument that section 8 of the Charter could be applied to create private rights between employer and employee. This leaves the conclusion that "...the union must base its grievance on an alleged contravention of some provision of the collective agreement and that it cannot rely on a generalised assertion that there is a free-standing right of privacy to justify its request for the removal of the internal cameras." Applying this strict contractual approach, Armstrong does go on to decide that connecting the cameras without clear and convincing evidence of why this was required would be an unreasonable exercise of management rights under the agreement. However, if the wording of the collective agreement had not placed limitations on management rights, it appears that the surveillance would have been allowed irrespective of the severity of the effect on employee privacy.

The case of Re Hercules Moulded Products Inc and United Food and Commercial Workers

410 Ibid. at 80.
411 Ibid. at 81 and 84.
412 Ibid. at 86.
413 Ibid. at 85.
International Union ("Re Hercules"), the employer sought to rely on evidence gathered by video cameras hidden in the workplace in justifying the dismissal and discipline of a number of employees for misconduct. Arbitrator Criljenica rejected the union’s arguments about privacy, finding that there was no general right to privacy in Ontario, and Charter values were not applicable to private labour disputes. In considering the specific question of privacy in the workplace, Criljenica took the view that, in relation to surveillance at least, employees could not expect privacy when at work:

"To whatever extent such a right (or 'expectation') has been held to exist in regard to employer surveillance of off-duty activities of employees, or in regard to locker or lunch pail searches, it cannot possibly exist in regard to an employee’s activities on the work floor, where the employee must recognise that he or she may be observed by supervisors, leadhands or other bargaining unit employees."

The arbitrator in this case therefore appears to be taking an approach which denies employees any right to information privacy when they are actually in the workplace, on the basis that they might in any event be observed by supervisors and co-workers. However, as discussed in section 1.3 of chapter one, a right of information privacy can be applicable in the workplace even if employees expect to be supervised – electronic monitoring, whether by video or computer, is a cause for concern because of its potentially covert and pervasive nature. This is also recognised by the Supreme Court of Canada in R v Duarte, who distinguish electronic surveillance from the more general risk that our words might be overheard and repeated. This arbitration decision illustrates again the tendency to allow employers to manage and run their own workplaces as they see fit, irrespective of the effects on employee privacy.

Overall, it can be said that the application of privacy rights in arbitrations concerning workplace video surveillance has had somewhat mixed results. A number of the cases

---

414 *Ibid.* at 88. It had been found at the preliminary award in this case that the terms of the collective agreement did require that workplace rules be “reasonable” and that management rights be exercised in a reasonable manner: (1999), 80 L.A.C. (4th) 426 (Armstrong, Ontario) (preliminary award).


416 *Ibid.* at 184-185. It should be noted that he went on to find that the evidence should nevertheless be subject to a test of reasonableness, on the basis of his discretion under the Labour Relations Act 1995 and the “purpose” clause of the relevant collective agreement.

explicitly recognise that employees can have a right of privacy in these circumstances, and use a balancing test in weighing the effect on employee privacy against the employer's justification for the surveillance and proportionality of the employer's conduct. There does, however, remain a degree of emphasis on whether or not the surveillance was "covert" – showing a continuing preoccupation with the extent to which invasions of privacy are expected. There is also an alternative approach in some arbitrations, which shows a reliance on the strict wording of the collective agreement in question and the employer's right to run the workplace, and does not recognise privacy as an external value which is relevant to the labour relationship at all. Despite these limitations, the approach taken in those cases which are more sympathetic towards employee privacy rights could certainly be extended to cases of e-mail and internet monitoring, where the interests at stake are substantially the same. This would seem to be preferable to the approach taken in the few arbitrations about computer monitoring which have been decided to date, which fail to give workplace information privacy genuine recognition.

3.5 Conclusions

Looking at the overall picture of privacy in relation to workplace e-mail and internet use, it is clear that no one coherent approach emerges from Canadian law. The present state of the law can be summarised as follows.

In relation to legislation, the most striking feature is the fact that the relevant statutes are so piecemeal in their application. The extent of workplace privacy protection afforded by Canadian legislation largely depends on whether the employment in question is federally or provincially regulated, public or private, and on the province in which the employment is based. The various different pieces of legislation also differ in their scope and approach towards defining privacy, and none of the legislation is designed to apply explicitly to the employment relationship. However, it can be said that a couple of common principles do emerge from an analysis of the relevant legislation. First, the concept of consent appears to

418 Supra note 338.
be important, appearing in the Criminal Code, PIPEDA, and the various provincial Privacy Acts. Secondly, some of the legislation requires consideration of the "reasonableness" of the employer's purposes and/or overall conduct – this concept is used in PIPEDA and some of the provincial legislation, and emphasised by both the PCC and Ontario IPC. These themes will be explored further in the next chapter.

In relation to application of privacy principles in caselaw, the Charter has been interpreted as including a right of privacy which is directly applicable to the question of electronic monitoring. However, there remains a query about the interpretation of reasonable expectations of privacy and the extent to which the right is protected if invasions are expected, and again the Charter has direct application only to public sector employees. The application of privacy principles in the private sector employment context is illustrated by some of the arbitrations dealing with workplace video surveillance, which show that there is scope for recognition that any surveillance by an employer can affect employee privacy interests. On the basis of a number of these decisions, it can be argued that the employer’s reasons for monitoring and the way in which that monitoring is carried out should be weighed in all cases against the effect on employee privacy. However, these decisions only apply to unionised employees, and to date privacy has not been used to any effect in the common law employment relationship. Even in grievance arbitration jurisprudence, there remain some conflicting approaches which go so far as to deny the existence of information privacy rights within the workplace. Perhaps most significantly, when the issue of employee privacy is considered in the precise context of employer computer and e-mail monitoring, arbitrators appear to fall back on a limited view of expectations of privacy in the workplace which emphasises the ability of the employer to control those expectations. As is the case with UK law, there is a clear trend towards recognition of the employer's management prerogative to supervise and control the workplace in protection of its own interests, at the expense of meaningful employee privacy rights.

The law in Canada is more developed in this area than the law in the UK, where such issues are only starting to be considered in light of the new legislation described in chapter two. Canadian law does provide some concrete (although somewhat conflicting) examples of how
privacy rights can be used in the context of employer surveillance of employees within the workplace. However, as with the UK legislation, Canadian legislation and caselaw exhibits a variety of different approaches and levels of recognition of workplace privacy rights. The problems with some of these approaches towards information privacy, together with the possible reasons behind them, will be considered further in the following two chapters.
4 PRIVACY AND THE EMPLOYMENT RELATIONSHIP

"Their actions are watched: their conversations, computers and correspondence monitored; their personalities assessed; their bodies poked, prodded and drained. Their physical integrity and private behaviours are sacrificed on the employment altar. Only the limits of technology, limits that are fast receding, and a string of incomplete and inadequate laws, prevent even more intrusive surveillance." (Eugene Oscapella).\(^{419}\)

The preceding two chapters have provided a comprehensive outline of the UK and Canadian approaches towards privacy in the context of workplace e-mail and internet monitoring. This chapter aims to pull together the themes which have emerged from the study of the law in these two jurisdictions, and draws on these themes in considering the wider question of why protection of information privacy within the employment relationship appears to be particularly problematic. It was established in section 1.2 of chapter one that, although it may have its costs, privacy is a right which serves important values in today’s society and requires genuine protection. However, information privacy in the workplace is given insufficient recognition. Various theories of the relationship between employer and employee will be discussed and applied to the issue of workplace privacy. It will be seen that approaches which rely on “reasonable expectations” of privacy and/or consent provide inadequate protection to employees by giving the employer too much power to control the scope of employee rights. This is a problem because of the dynamics of the employment relationship itself, and because of the importance of privacy within that relationship. This in turn shows a trend amongst both courts and legislators to rely on an analysis of the employment relationship which is based on freedom of contract and the employer’s prerogative to control the workplace, rather than recognising privacy as a right which operates irrespective of the contract between the parties.

It should be noted at this point that this chapter does not try to provide a complete critique of approaches towards the definition of privacy rights in UK and Canadian law. It may well be that there are wider problems with concepts which are relied on in relation to privacy, such as the ideas of reasonable expectations and consent, so that some of the criticisms of workplace

\(^{419}\) Oscapella (1998) supra note 51 at 341.
privacy law could apply equally to privacy law in general. However, such issues are beyond the scope of this thesis. The focus of this chapter is on privacy in the specific context of the workplace. Very particular problems are caused when privacy definitions interact with the employment relationship, meaning that privacy “fails” in a workplace setting when it might not do so elsewhere. It is therefore the combination of these two factors which is the focus of the following discussion.

Before looking at the specific question of definitions of privacy, it will be helpful to carry out a brief overview of theoretical approaches towards the employer/employee relationship in the UK and Canada. The aim is to show how fundamental human rights such as privacy can and should be applied within an employment relationship. This theoretical framework will provide the basis for a discussion of whether the common themes relating to privacy which appear in UK and Canadian law do in practice provide appropriate protection of workplace privacy rights.

4.1 The employment relationship in the UK and Canada

The relationship between employer and employee in both the UK and North America has traditionally been seen as a matter of freedom of contract. Both parties are left to bargain over the terms and conditions governing the relationship between them without external legal intervention. The law has assumed that the employment contract is an agreement between equals, negotiated to suit the interests of both parties. This approach would leave the question of rights in the workplace, such as privacy rights, as a matter of negotiation between employer and employee.

However, it has increasingly been recognised that there may be justifications for placing restrictions on pure freedom of contract in the sphere of employment, based on concerns about the inequality of bargaining power between the parties. It is argued that in reality an individual employee has no equality of bargaining power as compared to a powerful

---

employer, resulting in terms and conditions of employment effectively being imposed on the individual rather than negotiated.\textsuperscript{421} This view was perhaps most famously expounded by Otto Kahn-Freund, who described the employment relationship as follows:

"...the relation between an employer and an isolated employee or worker is typically a relation between a bearer of power and one who is not a bearer of power. In its inception it is an act of submission, in its operation it is a condition of subordination, however much the submission and the subordination may be concealed by that indispensable figment of the legal mind known as the 'contract of employment'."\textsuperscript{422}

An approach which recognises the imbalance of power between the parties to an employment contract allows external restraints to be placed on the bargain which may be agreed between the parties. Although this limits freedom of contract, it can be seen as necessary to protect individual freedom, providing protection from oppression and the employer's unconstrained power.\textsuperscript{423} It is a way of restoring some measure of equality between the parties. Labour law effectively operates as this "countervailing force", counteracting the imbalance of power which is inherent in the employment relationship.\textsuperscript{424} As recognised by Bora Laskin in 1938, limitations on freedom of contract can in fact "enlarge the liberty of men".\textsuperscript{425} Such limitations "...bear witness to the fact that there resides in the community a power to restrict the freedom of individuals to contract, when such freedom in fact destroys the interests of the individual."\textsuperscript{426} Freedom in the workplace can effectively be described as the employer's freedom from state control; for most employees, their only freedom is to leave an intrusive or constrained workplace.\textsuperscript{427}

One way of addressing this imbalance of power between an employer and an individual employee was to rely on collective labour law. Collective bargaining was seen as the best way to modify the inherent inequality of bargaining power, coupled with a resistance to

\textsuperscript{421} Ibid. at 6 and 106-107.
\textsuperscript{422} O. Kahn-Freund, \textit{Labour and the Law} in P. Davies and M. Freedland, 3\textsuperscript{rd} ed., (London: Stevens and Sons) at 18.
\textsuperscript{423} Ibid. at 24 and 25.
\textsuperscript{424} Ibid. at 18.
\textsuperscript{426} Ibid. at 675.
\textsuperscript{427} Finkin (1996) \textit{supra} note 54 at 255.
external legal interference between the parties.\textsuperscript{428} The theory of "collective laissez-faire" protected freedom of contract while also providing protection for the individual by means of collective bargaining.\textsuperscript{429} Legal abstentionism allowed the parties to regulate their own activities, with workplace relationships being governed by social rather than legal rules.\textsuperscript{430}

However, even exponents of collective laissez-faire recognised that some external regulatory legislation relating to the individual employment relationship might be required, to fill the "gaps" which might be left by collective bargaining. The purely voluntary system of collective laissez-faire could be criticised as failing to provide protection for the individual employee. This can be argued on the basis that collective bargaining did not provide comprehensive protection for types of employee who were not traditionally unionised, and also on the basis that collective bargaining was under the control of employers and unions rather than conferring an entitlement on individuals and therefore might fail to protect individual rights adequately.\textsuperscript{431} One way of addressing this problem is to provide a minimum "floor of rights", which do not form part of the contract of employment and can not be departed from by agreement, but which can be built on by collective bargaining.\textsuperscript{432} This approach does not challenge the fundamental premise that the individual employment relationship should primarily be regulated through collective bargaining, but can be criticised as not going far enough. Taking the example of discrimination law, the collective bargaining process itself may be inherently discriminatory - in order to provide adequate protection for individuals the law needs to be more interventionist, cutting across established industrial practices rather than simply fitting around the existing system of collective bargaining.\textsuperscript{433} This focus on "industrial justice" led to labour legislation which regulated the individual employment relationship, such as discrimination law, health and safety legislation, and protection against unfair dismissal, the state thereby intervening in parties' ability to define the terms of their own relationship.

\textsuperscript{428} Wedderburn (1986) supra note 420 at 16 and 106-107.
\textsuperscript{430} \textit{Ibid.} at 9.
\textsuperscript{431} \textit{Ibid.} at 52.
\textsuperscript{432} See for example Wedderburn (1986) supra note 420 at 5-6.
The introduction of a right to privacy within the employment relationship, a value imposed by the state which is not dependant on individual or collective negotiation, is a further example of a industrial justice approach to labour law. This clearly does undermine the principle of free collective bargaining. Some commentators argue that this approach is inappropriate, noting for example that the matter of workplace privacy should be treated as "...a private issue between the parties to the collective agreement rather than as an exercise in public policy". It can further be argued that in cases of dispute this approach allows arbitrators to fashion solutions which are suitable to the specific workplace - "It is this decentralising notion which has always been the bedrock of free collective bargaining." However, the limitations on free collective bargaining which are inherent in an industrial justice approach can be justified on the basis that some rights are so fundamental that they should not be subject to "concession bargaining" and potentially traded-off for other collectively-negotiated rights. The subordination of individual rights to economic goals is a real possibility if the existence of such rights is entirely dependant on collective negotiation, and it can be argued that this is particularly problematic where a recognised human right such as privacy is at stake.

The need to intervene in the employment relationship to redress the inherent imbalance of power between the parties has been explicitly recognised by the Supreme Court of Canada in two cases. In *Slaight Communications Inc v. Davidson*, the Court decided that the Charter could not be used by an employer to challenge an adjudicator’s order in favour of an employee. The majority decided this in part on the basis that the order was justified because it was aimed at protecting a particularly vulnerable group, namely employees. Dickson CJ quoted the observations of Kahn-Freund set out above, and described the adjudicator’s remedy as "...a legislatively-sanctioned attempt to remedy the unequal balance of power that normally exists between an employer and employee." He also took the view that protecting the employer’s constitutional rights in this case "...would be tantamount to

---

435 Ibid.
436 Morris (2001) *supra* note 175 at 68.
condoning the continuation of an abuse of an already unequal relationship.\textsuperscript{440} The majority of the Court in this case therefore saw the imbalance of power as so strong that it justified overriding the employer's rights under the \textit{Charter}. In the subsequent case of \textit{Wallace -v- United Grain Growers Limited},\textsuperscript{441} the Supreme Court noted that the power imbalance between the parties was not simply limited to the employment contract, but "...informs virtually all facets of the employment relationship."\textsuperscript{442} The Court again noted the particular vulnerability of employees, and relied on this in finding that failure to treat employees reasonably and decently at the time of dismissal would justify adding to the length of the employee's notice period.\textsuperscript{443} Neither of these cases relates directly to the issue of employee-protective legislation overriding the provisions of an employment contract. However, they do show that the Supreme Court regards the imbalance of power between employer and employee as a weighty consideration which makes employees deserving of legal protection, a principle which can equally be applied to mitigate the effects of a strict freedom of contract analysis.

The industrial justice approach to labour law, which clearly limits the parties' freedom of contract, has been challenged by economic and market theorists.\textsuperscript{444} They argue that the employment relationship can be treated in the same way as any other commercial transaction, and there is not in fact a real imbalance of power between the parties. Put in simplistic terms, it is argued that efficiency will be maximised if workers are treated as consumers in an unregulated labour market, free to choose from a variety of jobs, employers, and terms and conditions of employment. Employers will be damaged if employees refuse to join or leave employment due to unacceptable terms and conditions, and therefore a mutually acceptable voluntary bargain can be reached between employer and employee. Freedom of contract is seen as the best way to maximise productivity and efficiency, and external legal regulation of such transactions introduces inefficiencies into the process. A version of this approach can

\textsuperscript{439} \textit{Ibid.} at 423.
\textsuperscript{440} \textit{Ibid.} at 424.
\textsuperscript{441} \textit{Supra} note 353.
\textsuperscript{442} \textit{Ibid.} at 32 per Iacobucci J.
\textsuperscript{443} \textit{Ibid.} at 37-38.
\textsuperscript{444} For a prime example of this approach see R. Epstein, \textit{Forbidden Grounds: the case against employment discrimination laws} (Cambridge, Mass: Harvard University Press, 1992), who argues that
be seen in UK labour law in the 1980s, where policies of de-regulation and flexibility were pursued in an attempt to turn the labour market into a free-market economy. This would leave no room for the imposition of external values such as privacy into the relationship. Individual employees and employers would be left to bargain freely about workplace privacy rights, and the most efficient outcome would thereby be reached.

The law and economics perspective of labour law has been heavily criticised for failing to recognise that there are key differences between the labour and the consumer market. For example, Weiler has pointed out a number of problems with this approach. He argues that it fails to recognise the human element. Even if efficiency is maximised in the long run, the approach inflicts immediate and severe distress on individual workers and their families, and there may be practices which are so damaging to human dignity that public policy requires limits to be placed on bargaining. It can also be argued that there is still an imbalance of power between employer and employee, so that it is more costly for employees to stand up for their rights. Modern employment often encourages an enduring career relationship by providing service-related advantages, making it increasingly damaging for employees to leave their employment if dissatisfied with their treatment as they get “locked into” their jobs. Workers may also be inhibited from freely changing jobs within the market by fear of unemployment, financial and relocation difficulties, and contractual restrictions. With specific reference to privacy, although employees who demanded privacy could lower the cost of their labour and thereby make it economically efficient for employers to ensure a privacy-protective workplace, it can be argued that it is unjust to require employees who desire privacy to be financially penalised for acquiring this right, and distasteful to set up a competition between those employees and others who are willing to give up privacy rights in return for higher wages. A purely market-orientated approach to the employment relationship has been rejected in both the UK and Canada. For example, in the UK, despite

anti-discrimination laws should be repealed on the basis that the free market rather than legislation is the best way to address discrimination in the workplace.

Davies & Freedland (1993) supra note 429 at 528.


Ibid. at 21-22.

Craig (1999) supra note 16 at 48-49.

Ibid. at 49.
the move in the 1980s and early 1990s towards an unregulated labour market based on individual negotiation, European Community labour law has operated to place social policy restraints on de-regulation – both because the denial of basic social standards seemed unacceptable to many member states, and in order to avoid the competitive threat of “social dumping” whereby states with minimal regulation of labour law would gain a competitive advantage over states with more costly worker-protective laws.\(^{450}\)

Some commentators have nevertheless argued that individual rights and freedoms may hold less sway in the workplace than elsewhere. In the context of industrial discipline and grievance arbitrations, George Adams has classified the workplace as a “special purpose community” with the prime purpose of maintaining efficiency and productivity, such that there may be less room for individual freedom than outside the workplace.\(^{451}\) The employer’s interests are based on the need for efficiency rather than the moral well-being of employees, and therefore he sees it as necessary to harmonise individual freedoms “taken for granted” outside the workplace with an employee’s position within an industrial relations community.\(^{452}\) This approach builds on Harry Arthurs’ concept of “industrial citizenship”, where employees are seen as having certain rights and duties as a result of being members of the industrial community rather than simply through contract.\(^{453}\) These approaches do still emphasise that contract alone is not sufficient to define the terms of an employment relationship, and employees may have rights which should not be destroyed by an employer’s superior bargaining power.\(^{454}\) This is therefore not inconsistent with a conception of fundamental employee rights, but rather recognises that employers may have their own interests which must also be considered. As discussed in section 1.5 of chapter one, privacy in the workplace certainly has costs for an employer, and these must be borne in mind when individual privacy is being protected. However, this weighing of recognised competing interests is very different from an outright denial of rights in the employment contract itself.

\(^{450}\) See Davies & Freedland (1993) supra note 429 at 590-599 and 661.

\(^{451}\) G. Adams, Grievance Arbitration of Discharge Cases (Kingston, Ontario: Industrial Relations Centre, Queen’s University, 1978) at 6.

\(^{452}\) Ibid. at 17 and 19-20.

Modern labour law therefore recognises that the demands of industrial justice require at least some external limitations to be placed on the negotiation of an employment contract. Protective legislation operates to secure certain basic employee rights, and often this is based on moral principles rather than economic efficiency—"The community proclaims that simple respect for the humanity of the worker requires a modicum of decent treatment on the job, and that this right is to be enjoyed equally by all workers, whatever their personal resources." An essential component of this approach appears to be that it should not be possible to "contract-out" of these rights. The issue of contracting-out can be seen as a question of how far individual rights which are secured by legislation can be voluntarily renounced by an individual. It can be argued that this depends on whether the claims of society, which has enacted such protective legislation, would forbid renunciation of those rights—which may require consideration of the policy behind the relevant statute.

In the context of worker-protective labour laws, which have been enacted at least in part to address the inequality of bargaining power between employer and employee, it seems clear that contracting-out should not be permissible. It would seemingly defeat the purpose of such legislation if employees could "negotiate" away their rights in an employment contract. It can further be argued that some rights are so fundamental to a democratic society that they should not be subject to exclusion by agreement, and also that such rights benefit the community at large as well as the individual, such that waiver of those rights would be contrary to public policy. A good example of this is human rights legislation prohibiting discrimination in employment, which can be seen as a recognition that "employees have employment rights that are not deferrable to mere private contractual interests". In both the UK and Canada, these rights can not be removed by the employment contract. It can be argued that other human rights which are applicable to the employment relationship should similarly be immune to waiver, such as freedom of association, freedom of

---

454 Ibid. at 787.
456 Laskin (1938) supra note 425 at 676.
457 Ibid. at 677.
458 Morris (2001) supra note 175 at 54-55.
459 P. Barnacle, Arbitration of Discharge Grievances in Ontario - Outcomes and Reinstatement Experiences (Kingston, Ontario: Industrial Relations Centre, Queen’s University, 1991) at 13.
expression, and also privacy. This approach towards freedom of expression in the UK is shown by the *Public Interest Disclosure Act 1998*,\(^{461}\) which protects employees who make disclosures about their employers which are deemed to be in the public interest.\(^{462}\) Not only is it impermissible to contract out of this legislation generally, but an individual can not contract-out of making a specific disclosure.\(^{463}\) It is strongly arguable that privacy, a right protected alongside freedom of expression by the HRA in the UK and the *Charter* in Canada, should be treated in the same way.

The application of privacy to the employment relationship will now be examined in light of this theoretical background, with specific reference to the power of employers to dictate the terms of the relationship and the issue of contracting-out.

**4.2 The problem of contracting-out of privacy rights**

Privacy can be seen as a fundamental employee right which should not be susceptible to waiver by agreement in the employment contract. It is a value imposed on the employment relationship externally, safeguarding important individual and societal interests that should not be threatened by an employer’s superior bargaining power. At first sight, this is the approach towards information privacy in the workplace which appears to be taken by both UK and Canadian law. In the UK, the HRA guarantees certain fundamental rights to all employees.

---


\(^{462}\) *Public Interest Disclosure Act 1998* c23.

\(^{463}\) The Act provides that “qualifying disclosures” made by workers in specific circumstances will be protected, so that the employer is prevented from dismissing workers or subjecting them to any other detriment as a result of the disclosure. Qualifying disclosures are those relating to a specific list of subjects, including those about criminal offences, failures of legal obligations, miscarriages of justice, health and safety, and the environment (set out in section 1). There is a strict procedure set out about the persons to whom disclosures must be made, starting where possible with the employer and/or the relevant regulatory body (see section 1).

\(^{464}\) Part 43J of section 1 provides that “(1) Any provision in an agreement to which this section applies is void in so far as it purports to preclude the worker from making a protected disclosure. (2) This section applies to any agreement between a worker and his employer (whether a worker’s contract or not), including an agreement to refrain from instituting or continuing any proceedings under this Act or any proceedings for breach of contract.” This means that an explicit contractual term can not prevent a worker from making a protected disclosure, and this even applies to agreements in settlement of claims under the Act (whereas under most UK employment legislation, settlement agreements are an exemption to the usual rule about contracting out).
citizens which should not be excluded by agreement. RIPA and the DPA are regulatory statutes which operate outside the employment contract. Similarly, in Canada privacy values guaranteed by the Charter can be imposed on the employment relationship, and the various pieces of privacy-protective legislation are applied irrespective of the parties’ contractual intentions.

However, although privacy appears to be a right which can not be contracted-out of by the parties, the way in which privacy operates in practice in the context of an employment relationship tends to undermine this approach. Even if direct contracting-out is not allowed, the same effect seems to occur when privacy is applied in the workplace due to the way in which privacy itself is defined. This can be illustrated by two themes which have emerged from the discussion of UK and Canadian law in the context of e-mail and internet monitoring, namely reasonable expectations of privacy, and consent.

4.2.1 Contracting-out and reasonable expectations of privacy

Both UK and Canadian law in some contexts only provide protection of privacy rights if an individual is found to have a “reasonable expectation” of privacy. This concept is not clearly defined in either jurisdiction, but where it is applied it is a crucial precondition to the existence of a privacy right. It appears that this can be either a normative concept, based on general societal expectations of privacy, or an empirical concept, based on what an individual has actually been led to believe in specific circumstances.

In the UK, the requirement that an individual has a reasonable expectation of privacy is essential to protection of the right to respect for private and family life under the HRA. As discussed in detail in section 2.2.2 of chapter two, in applying this right under the Convention in the Halford case, the ECHR clearly takes the approach that a reasonable expectation of privacy

---

464 It should be noted that this is not explicitly clear in the legislation, and some caselaw from the ECHR suggests that Convention rights can be subject to an unequivocal waiver – although it is perhaps to be doubted whether the HRA will be treated in the same way, and there are also arguments as to why waivers should not operate in the employment context. For a more detailed discussion see Morris (2001) supra note 175.

465 Supra note 151.
privacy is a required precondition to the existence of a right to privacy. Without such an expectation, considerations of the employer's reasons for monitoring do not even arise, as no privacy right has been infringed. Although the case is not explicit about the test for reasonable expectations, it can be inferred from the judgement that the question turns on what the individual has been led to believe in the relevant circumstances. This suggests that the test is an empirical one, which depends on the facts of the individual case.

Canadian law similarly relies on reasonable expectations of privacy. This is particularly clear from the general Charter jurisprudence on surveillance and privacy, discussed in section 3.2 of chapter three. Although some of the caselaw seems slightly contradictory, it appears that the correct approach is similar to that of the ECHR and the HRA, namely that of requiring a reasonable expectation of privacy to exist before a privacy right will be protected by the Charter. As previously discussed, it is somewhat unclear whether expectations of privacy depend on the individual's actual understanding in specific circumstances, or whether the concept is based on wider expectations of appropriate levels of protection in a free and open society. The latter approach is suggested by the majority judgement in R v. Wong, where the test is expressly related to society's values and therefore appears to be a normative one. However, an emphasis elsewhere in the caselaw on surreptitious surveillance suggests that the test can also be an empirical one, as under the HRA.

The requirement for there to be a reasonable expectation of privacy appears elsewhere in Canadian privacy law. The Criminal Code defines a private communication as one made in circumstances where it is reasonable to expect that it will not be intercepted - seemingly an empirical test depending on the facts of the case. With specific reference to the workplace, a number of grievance arbitrations have also taken this approach. This is most marked in the arbitrations dealing directly with e-mail and computer monitoring. In both of the relevant cases discussed in chapter three, the arbitrators concentrated on the individual employee's expectations of privacy in the circumstances of the case. Neither employee had been led to believe by their employer that use of the workplace computer equipment would be private,

---

466 Supra note 344.
467 See section 3.1.1 of chapter three.
468 See section 3.4.1 of chapter three.
and therefore neither employee had a privacy right. Again, this is applying an empirical test of reasonable expectations. A similar view is suggested by some of the grievance arbitrations dealing with workplace video surveillance. In both St Mary's\textsuperscript{469} and Re Brewer's Retail.\textsuperscript{470} the arbitrator emphasises the particular dangers of covert surveillance, and it is suggested that surveillance which is known about by employees presents less of a threat to individual privacy.\textsuperscript{471} This in turn suggests that expectations of privacy may depend on whether the individual was aware that workplace conduct might not be private. Although these two arbitrations do not go so far as to treat a factual expectation of privacy as an essential precondition to a privacy right, this is nevertheless seen as an important consideration in deciding the strength of the individual's claim to privacy protection.

Overall, both UK and Canadian law seem to favour an empirical test of reasonable expectations of privacy. This is particularly significant when applied to the employment relationship. If an individual's expectation of privacy is an empirical question, the employer has power to dictate the levels of privacy which can be expected in a particular workplace. It seems that the scope of an individual's privacy right is capable of being "shaped by contract".\textsuperscript{472} An employment contract could simply specify that employees have no expectations of privacy over, for example, e-mail and internet use in the workplace. This would seemingly prevent a privacy right in relation to e-mail and internet use from arising at all. Although an employer can not insist on an employee contracting-out from privacy-protective legislation directly, the employer's power to define expectations of privacy in the employment contract has exactly the same effect. This appears to defeat the point of privacy rights which are ostensibly designed to protect employees irrespective of the employer's superior bargaining power. The reality for most employees is that such a provision in an employment contract is not a matter for negotiation – the individual either has to accept the limitations offered in the contract, or not be hired.

The difficulties with applying reasonable expectations of privacy to the employment

\footnotesize
\textsuperscript{469} Supra note 396.
\textsuperscript{470} Supra note 402.
\textsuperscript{471} See section 3.4.2 of chapter three.
\textsuperscript{472} See Morris (2001) supra note 175 at 61 in relation to the right under the Convention.
relationship are in fact wider than simply that of contracting out. Not only can an employer set privacy expectations by contract, but it also appears that such expectations do not even require a notional "agreement" between the parties. It seems that an employer could define employee privacy expectations unilaterally, by introducing a policy about workplace privacy, or arguably even by a simple warning that certain conduct will not be treated as private – anything which alters an individual's factual expectations is enough. This effectively makes workplace privacy a matter of self-regulation by employers. This can be seen as an unacceptable way to deal with employee privacy rights as it results in employer interests being given priority, particularly in the face of the increase in potentially invasive employer practices such as e-mail monitoring.\textsuperscript{473} The emphasis on employee expectations of privacy can be criticised as it "...essentially guarantees no absolute protection for employees because employees' expectations are increasingly compromised by developing technology, newly conceived employer interests, and expansive employer monitoring policies."\textsuperscript{474}

Determination of expectations of privacy in this way simply means that the concept rests on employer policies, practices or assurances.\textsuperscript{475} As Finkin has noted, established business practice in relation to expectations of privacy is likely to be relied on even where the individual employer in question does not have its own standards in place – in looking for external norms, the courts will tend to fall back on what can generally be expected in the workplace.\textsuperscript{476} If workplace privacy standards can generally be set by employers, the danger is that these standards will invariably favour employer interests over individual privacy, and will also become the "norm" to be expected in workplaces which do not have explicit privacy-related policies. This would result in expectations of privacy in the workplace being defined according to employer needs and interests. This hardly seems appropriate for a right which is theoretically given such importance that it can not even be removed by agreement between the parties to an employment contract.

The limitations of this approach are perhaps most vividly illustrated by the two arbitration decisions on workplace computer use considered in section 3.4.1 of chapter three, namely


\textsuperscript{474} Ibid. at 411-412.

\textsuperscript{475} Finkin (1996) supra note 54 at 226.
International Association of Bridge$^{477}$ and Camosun College.$^{478}$ In both of these cases, the arbitrators emphasised the grievors' knowledge that ostensibly "private" files and e-mails could be accessed by the employer. This knowledge meant that the grievors had no expectation of privacy, and therefore no privacy rights over the material in question – even though, in the case of International Association of Bridge, the grievor had tried to protect some of the material with a private password. The employers in these cases were able to defeat employee privacy expectations simply by maintaining a computer system which was not intrinsically private. This requires even less from the employer than a contract or policy making it clear that such communications in the workplace will not be regarded as private. On the basis of these decisions, any factual circumstances which lead employees to believe that their communications might be seen by their employer will be enough to prevent privacy rights from arising at all.

Some might argue that a purely empirical definition of reasonable expectations of privacy is nevertheless appropriate, on the basis that a real threat to privacy does not arise if an individual is aware that potentially private activities might be being observed. In such circumstances an individual is able to modify behaviour accordingly and protect information which he or she does not want to be revealed – it is surreptitious surveillance and monitoring which poses the real threat. Certainly a number of the Canadian cases emphasise the particular dangers of covert surveillance. As discussed in section 3.2 of chapter three, comments by La Forest J in $R v$- Duarte$^{479}$ and $R v$- Wong$^{480}$ suggest that it is circumstances in which individuals do not expect to be watched or overheard which are particularly damaging. Similarly, the question of awareness of privacy-invasive surveillance is seen as important in the arbitration decisions of St Mary's Hospital$^{481}$ and Re Brewer's Retail,$^{482}$ where covert surveillance is treated as the practice most threatening to privacy rights.

$^{476}$Cited.
$^{477}$Supra note 372.
$^{478}$Supra note 378.
$^{479}$Supra note 338.
$^{480}$Supra note 344.
$^{481}$Supra note 344.
$^{482}$Supra note 396.
It is beyond the scope of this thesis to consider the general question of the definition of privacy in detail. However, at least in the context of the workplace if not elsewhere, it can briefly be explained why privacy rights can be regarded as infringed even if an individual knows that he or she is being observed. Firstly, it is simply extremely difficult if not impossible for individuals to deal psychologically with the effects of being under constant surveillance. As referred to in chapter one, Westin has argued that the human psychological need for privacy is essential to the effective operation of social structure, and total surveillance can not be tolerated by most people. It can further be argued that the values served by privacy can be implicated as much by open as by covert invasions of privacy. As discussed in section 1.4.2 of chapter one, in the context of e-mail and internet monitoring, privacy interests can be affected by the mere threat than one might be being observed. The power of the Panopticon lies in the fact that the prisoners are aware that they could be observed, but are not sure at any one time whether they are actually subject to surveillance. It is this knowledge of the possibility of observation which has an inhibitory effect on conduct. Similarly, the values served by privacy such as personal autonomy, furtherance of democracy, and personal wellbeing, are clearly endangered in circumstances where an individual is fully aware of being observed. Again, conduct furthering these values will be inhibited. Although it could be argued that individuals are free to act privately elsewhere, this limited conception of privacy rights is particularly troubling in the context of the modern workplace, where individuals spend a large amount of their time. If the values of autonomy, democracy and personal wellbeing are truly important to society, it seems undesirable that these values should not be adequately protected in the place where most adults spend a considerable proportion of their waking hours. It can also be argued that if the knowledge of surveillance results in expectations of privacy being lost, then privacy rights themselves will diminish over time as individuals become increasingly aware of surveillance capabilities and practice. The more privacy is removed by open surveillance practices, the less privacy can be expected by individuals, and therefore ultimately the scope of privacy rights could be reduced to virtually nothing. This appears to be a real danger of approaches which treat expectations of privacy as a purely empirical concept, rather than taking a normative

\footnotesize
\begin{itemize}
  \item ^{482} Supra note 402.
  \item ^{483} Westin (1967) supra note 9 at 58-59.
  \item ^{484} Craig (1997) supra note 357 at 396.
\end{itemize}
perspective based on the expectations of society as a whole.

It can therefore be seen that an approach towards expectations of privacy which is based on an individual's state of knowledge of potentially privacy-invasive practices fails to provide comprehensive protection of employee privacy interests. Not only does this allow for effective "contracting-out" of the right of privacy, but employers also appear to have the power to define privacy expectations unilaterally, so setting the standard for workplace privacy on the basis of their own interests. This problem is caused by the combination of an empirical definition of expectations of privacy with the unequal balance of power in the employment relationship.

4.2.2 Contracting-out and consent

Consent to invasions of privacy is another theme which emerges from a study of UK and Canadian approaches to privacy. Both jurisdictions tend to treat consent by an individual as something which legitimises conduct which would otherwise be seen as privacy-invasive. In both jurisdictions, the idea of "consent" in the context of privacy appears in general legislation which is not directed specifically at the employment relationship. The basic concept is that, in the context of informational privacy at least, there is no threat to privacy interests if an individual has freely consented to divulge "private" information. The concern addressed here is the fact that, as with reasonable expectations of privacy, it is the application of the concept of consent to the employment relationship which causes particular difficulties for the protection of employee privacy.

In the UK, consent is important to the DPA. As outlined in section 2.4.1 of chapter two, consent is one of the preconditions which can be met in order to make data processing "fair and lawful". It is possible to raise some concerns about the use and meaning of consent in the DPA, particularly in the context of an employment relationship and in light of the DPA's departure from the more precise wording of the Directive on which it is based, an issue which has already been discussed at greater length in chapter two. RIPA similarly contains a provision whereby prior consent to the interception of a communication legitimises
potentially prohibited conduct.\textsuperscript{485}

In Canada, consent is also central to much of the privacy-protective legislation. PIPEDA is similar in its approach and scope to the DPA, and therefore similarly contains a provision requiring individual consent to the collection, use and disclosure of personal information.\textsuperscript{486} This consent must be "meaningful", although it does appear that implied consent is acceptable. The Criminal Code also contains a provision whereby liability can be avoided if the individual has consented to the relevant interception.\textsuperscript{487} Again, both express and implied consent are acceptable. Finally, the provincial privacy legislation in Saskatchewan, Newfoundland and Manitoba provides that both express and implied consent to potentially unlawful conduct will prevent such conduct from being an invasion of privacy.\textsuperscript{488}

Allowing an individual to consent to privacy-invasive practices effectively allows contracting-out of the right of privacy. Consent operates to prevent such conduct from being an invasion of privacy at all. Although the privacy-protective legislation itself in the UK and Canada can not be contracted-out of by agreement between the parties, the requirement of consent appears to have the same effect. In the context of an employment relationship, this raises the problems discussed above about inequality of bargaining power and the ability of employees to give up basic rights by "consent". Agreement to privacy-invasive practices in the workplace could simply be included as part of the contract of employment, so providing general "consent" at the outset of the relationship. Weiler gives the example of employee consent to random drug testing to illustrate the fact that a voluntary transaction between employer and employee may nevertheless be deemed undesirable. The transaction may seem economically sound, but if the practice is judged to be an affront to employee privacy and dignity, society may take the view that individuals should be protected from the temptation to agree to such practices in return for immediate benefits.\textsuperscript{489} If consent removes an employee's privacy rights, the temptation to agree to a privacy-restricted workplace clearly remains.

\begin{itemize}
\item \textsuperscript{485} See section 2.3 of chapter two.
\item \textsuperscript{486} See section 3.1.3 of chapter three.
\item \textsuperscript{487} See section 3.1.1 of chapter three.
\item \textsuperscript{488} See section 3.1.4 of chapter three.
\item \textsuperscript{489} See section 3.1.4 of chapter three.
\end{itemize}
A particular concern about employee consent in these circumstances is the extent to which such consent is free and genuine. Not only might employees be encouraged to agree to practices which are not in either their own or society’s best interests, but the dynamics of the employment relationship may mean that employees actually have no real choice but to agree to such measures. Again in the context of drug-testing, Finkin has pointed out that if ninety percent of Fortune 500 companies require a drug test as a condition of employment, consent to such a test is not truly free if the only alternative is relegation to a secondary labour market. An individual employee in these circumstances certainly has no power to negotiate alternative terms of employment. The choice is to consent to the test or take a job elsewhere, and the alternative options may become increasingly limited as drug testing becomes a standard industry practice and increasing numbers of employees “consent” to being tested in order to obtain the best jobs. A similar problem arises in relation to employee monitoring. Often consent to such monitoring will be required in the employment contract as a condition of being hired, and the individual’s only alternative to submitting to such privacy-invasive practices is to seek work elsewhere. In such circumstances, it may even be justified to describe consent to monitoring as almost always given under duress. This problem may also arise during the employment relationship, where an employer introduces a new workplace policy relating to privacy rights which requires employee consent. Again, employees may feel pressurised to consent to new practices which they are not comfortable with, either to avoid consequent limitations on their activities in the workplace (such as removal of the right to use e-mail and the internet if monitoring is not consented to), or even disciplinary sanctions. The reality of the workplace for most individual employees is that these issues can not be bargained over with the employer – they must either “consent” to invasions of privacy, or risk failure to be hired or even termination of employment. This imbalance of power was expressly recognised by the PCC in a recent speech about PIPEDA and workplace privacy. He emphasised that the “reasonableness” test under the Act showed that consent alone was not enough, so that even where consent was sought the proposed invasion of privacy still had to be appropriate under the circumstances – the playing

489 Weiler (1990) supra note 446 at 21.
490 Finkin (1996) supra note 54 at 256.
field is not always equal, and "fundamental rights can not be extorted away, or contracted away under duress."\(^{494}\)

The position is further complicated by the notion of implied consent within an employment relationship. As outlined above, much of the privacy-protective legislation in the UK and Canada appears to allow for implied consent. In the context of the workplace, consent might be implied in circumstances where the employee has not really addressed his or her mind to the issue, let alone provided free and informed consent. In relation to Canadian grievance arbitrations, a number of commentators have pointed out that consent to privacy-invasive practices might be implied from established past practice,\(^{495}\) or employee acquiescence in a new policy.\(^{496}\) Similarly, in the UK employees may be taken to have consented to a change in terms and conditions of employment, such as an alteration of privacy rights, by continuing to work after the change without complaint.\(^{497}\) This raises the possibility that explicit contracting-out by way of consent in the employment contract is not even required. Employees working in an organisation which already has a privacy policy may be taken to have consented to the policy by implication, simply because that policy has always been in place. Such an approach simply seems to entrench privacy-invasive practices which further employer interests at the expense of employee privacy. Similarly, an employer could introduce a new privacy policy into the workplace, which would be deemed to be accepted by the workforce unless one or more individuals are willing to complain and indicate that the policy is not accepted. This almost seems tantamount to removal of privacy rights by unilateral employer action, which hardly seems appropriate for a right which is theoretically so important that it is protected by legislation which can not be contracted-out of even by explicit agreement. A partial solution to this problem might be to approach the issue of implied consent from the perspective of a "reasonable person", judged on the basis of society's expectations of privacy.\(^{498}\) This would mean that consent would not be implied in

\(^{493}\) Supra note 72.
\(^{494}\) Ibid.
\(^{496}\) Bilsen (1992) supra note 65.
\(^{497}\) See further section 2.1 of chapter two and supra note 122.
\(^{498}\) Craig (1997) supra note 357 at 397.
circumstances where a reasonable person would expect to have their privacy protected, the assumption presumably being that individuals would not easily agree to such treatment. This would certainly help to alleviate the difficulties with implied consent. However, the expectations of a reasonable person would need to be based on society’s wider values rather than workplace-specific expectations which are likely to be inadequate in protecting privacy, and the more general problems with reliance on explicit consent would remain.

Finally, there is a question as to exactly what practices are being consented to. None of the UK or Canadian legislation makes it clear whether consent to each specific invasion of privacy is required, or whether a more general “blanket” consent is sufficient. If the latter, there may be further concerns as to whether employee privacy is being adequately protected. For example, in relation to e-mail and internet monitoring, an employer might require employees to consent to a general policy of computer monitoring without specifying the circumstances in which this may occur. Is such consent really adequate to cover all the potential types of monitoring which might take place, such as those discussed in section 1.4.1 of chapter one? It can be argued that consent to easily understood “routine” workplace observations does not equate to consent to more unusual and intrusive types of monitoring.

Although workers may expect some degree of monitoring by supervisors in the workplace, "...that is not to say that a “non-normal” observation of the individual – a search, for example – for which the worker has apparently given consent, is not an invasion of privacy.”

The introduction of consent into the question of privacy in the workplace is problematic in itself, as it equates to employee contracting-out of privacy rights. When this is coupled with concerns about the genuineness of consent in the context of the employment relationship, together with questions about the validity of implied consent and “blanket” consent, the concept seems to have a severe impact on employee privacy rights. As with reasonable expectations of privacy, power to dictate the level of privacy granted in the workplace appears to be left with the employer. Although consent to invasion of information privacy

499 Ibid.
500 Rigg (1991) supra note 360 at 86.
501 Ibid.
rights might make sense in some other contexts, when applied to the employment relationship it provides scope for employee privacy rights to be severely limited.

4.3 Why does contracting-out happen?

Reliance on reasonable expectations of privacy and consent in the context of the employment relationship operates to make employee information privacy rights effectively meaningless. Application of these concepts result in contracting-out of the right to privacy, and when this is coupled with the imbalance of power in the employer/employee relationship, workplace privacy becomes employer-regulated and so inadequately protected. The basic idea of industrial justice, which calls for external regulation of the bargain which can be negotiated between the parties, appears to collapse when these privacy definitions are applied in the workplace.

This result is very different from the treatment of other basic workplace rights. Employment standards such as minimum notice periods, hours of work, minimum wages, and health and safety standards, are set up by legislation to be immune from alteration by the employment contract. Similarly, fundamental human rights which apply both in the workplace and elsewhere can not be altered or avoided by agreement between two parties. In theory, privacy is another such fundamental right. As already discussed, both discrimination law and freedom of expression rights are clearly applicable within the employment relationship. They operate as an external limitation on the employment contract, on the basis that they safeguard rights which are important to society. Why is privacy treated differently?

One possible explanation is that privacy is seen as some kind of “second class” human right – although important, it can be susceptible to alteration or removal by agreement because it serves values which are less vital to society than those served by other rights such as equality and free expression. However, this does not seem to be the solution. Section 1.2.2 of chapter one has considered the values furthered by privacy. Autonomy, democracy and dignity can hardly be said to be unimportant goals, and they overlap with the goals of other fundamental
rights. Privacy is included in the Convention, the HRA and the Charter, with no indication that it should be regarded as less important than other protected rights. It could perhaps be argued that the right of privacy might be valuable elsewhere, but is of little applicability within the workplace. However, there are a number of strong arguments in support of recognition of the right of privacy in the workplace which relate back to the values served by privacy in general, as discussed in section 1.3 of chapter one. An approach which denies the existence of workplace privacy is simply not justifiable.

An alternative explanation is that the unsatisfactory protection of information privacy in much of UK and Canadian law is simply an unfortunate accident caused by the interaction of privacy concepts with the specific situation of the employment relationship, for which those concepts were never designed. Ideas such as reasonable expectations of privacy and consent function perfectly satisfactorily outside the employment context, and it is the dynamics of the employer/employee relationship which causes unforeseen problems. This is certainly a partial explanation of the situation. Much of the UK and Canadian law in question is not directed specifically at the workplace, and it is the imbalance of power between the parties to an employment contract which causes particular concern about “contracting-out”. These difficulties would not necessarily arise in other types of relationship.

However, the situation is more complex than this. Most fundamentally, the idea of contracting-out of human rights such as privacy can be regarded as a more general problem which is not limited to the employment context. Unfortunately it is beyond the scope of this thesis to consider this wider question, which raises some basic issues going back to the adequacy of the legal definition of privacy itself. However, other complexities also emerge. For the purposes of this study, the aspect of the interaction between privacy definitions and the employment relationship which is most interesting is the extent to which labour law has deliberately used basic privacy concepts to limit the scope of workplace privacy rights.

Both UK and Canadian law exhibit a particular reluctance to prioritise privacy rights over employer needs and interests. Ideas such as reasonable expectations of privacy and consent are certainly problematic in themselves when applied in the workplace. However, although
in both jurisdictions examples of application of these concepts are somewhat limited, there is a common theme that they are used to defeat rather than enhance privacy claims. This is particularly the case with information privacy rights, where there is a tendency for the law to fall back on notions of freedom of contract and the employer’s prerogative when such rights are at stake in the workplace. The prevailing approach is to subordinate employee information privacy rights to employer interests, showing an underlying attitude towards the employment relationship which treats such rights as a matter of private ordering. Some examples from both the UK and Canada can be used to illustrate this point.

In both of the Canadian grievance arbitration decisions dealing directly with the question of computer monitoring,502 the arbitrators took a very limited view of workplace expectations of privacy, finding that there were no privacy expectations if individuals were aware that their documents could be accessed by their employer. Although these decisions could be seen as constrained to some extent by the doctrine of reasonable expectations of privacy, this concept could have been used in a way which was more protective of employee rights – if not by adopting the normative approach suggested by some of the Supreme Court Charter decisions, then at least by requiring the employer to have actually informed employees that monitoring would take place. By adopting this limited approach, the subtext of these decisions is that the employer has complete prerogative to control use of its computer system, and employees have no expectation of privacy unless there is a contractual term to this effect. Some of the arbitration decisions concerning workplace video surveillance are more protective of employees. However, the cases of Re QBD Cooling Systems and Re Lenworth show arbitrators relying solely on the terms of the contract between the parties. The most recent decision in Hercules503 goes so far as to deny any right to information privacy when an employee is at work and can be observed by others. The few examples of circumstances in which provincial Privacy Acts have been applied in the workplace continue this theme. In UFCW Local 1400,504 the court emphasised the employer’s prerogative to defend its own property. In Richardson,505 the court went further and denied that an employee could have a

502 International Association of Bridge supra note 372, and Camosun College supra note 378.
503 Supra note 415.
504 Supra note 307.
505 Supra note 309.
privacy right when on company time and property. Again, the idea of expectations of privacy was given a limited interpretation in the context of an employment relationship.

In the UK, there are fewer examples of the application of information privacy in the sphere of employment. However, it can be seen that similar themes emerge. From the *Halford* case,506 it appears that the concept of expectations of privacy in the workplace context is to be treated as a question of whether or not the employer had allowed such expectations to arise, an empirical test controlled by the employer’s conduct. This limited interpretation of privacy rights is something which might well not occur in the same way in a scenario involving invasion of information privacy by the state in its capacity as government rather than as employer. For example, if the facts of the *Halford* case involved a state interception of a private citizen’s telephone calls outside the workplace, it seems unlikely that the same empirical approach towards reasonable expectations of privacy would be adopted. Even if the interception was of a communication over a state-regulated system, and the state had issued warnings that interceptions might take place, it is strongly arguable that the practice would nevertheless be seen as infringing citizens’ rights to privacy. However, in the workplace, it seems that the employer is able to control the extent of information privacy. A similar deference towards employer interests is shown by the Lawful Business Practice Regulations in the UK.507 These Regulations were specifically adopted to address employer concerns about the limitations which RIPA would otherwise place on monitoring of computer use in the workplace. They operate as an exception to RIPA’s general consent requirement, and are seemingly designed to allow for monitoring in almost any circumstances thought necessary by the employer. Even the idea of the need to alter employee expectations of privacy is watered down to a requirement to make “reasonable efforts” to inform employees of potential monitoring. This is very significant as regulations altering the requirements of RIPA have not been adopted for any other sphere. It is only the workplace which is treated as a problem, where constraints on an employer’s ability to regulate the workplace are seen as unacceptable.

506 *Supra* note 151.
507 *Supra* note 177.
These examples show that when privacy concepts are applied in the context of an employment relationship, both UK and Canadian law exhibit a tendency to allow information privacy rights to be controlled by contract and the employer's business needs. This is more than simply the result of constraints imposed by the application of information privacy concepts drawn from the general law. Where an employment relationship is involved, these concepts are given a limited interpretation which emphasises the power of the employer to control the level of privacy applicable in the workplace and the terms and conditions of the relationship – a labour law approach which relies on freedom of contract rather than recognising privacy as a right which operates to constrain the employer's negotiating power. On the basis that privacy is a fundamental right on a par with other rights such as equality and freedom of expression, this approach fails to give employee information privacy the protection which it deserves.

The possible reasons why information privacy rights are vulnerable to a freedom of contract analysis, when other rights are not, will be considered further in the conclusion to this thesis. However, it will be helpful at this stage to consider if there is an alternative approach towards workplace privacy rights which is capable of giving such rights genuine recognition within an employment relationship.

4.4 Proportionality – the way forward?

As has been discussed in section 1.5 of chapter one, information privacy undoubtedly has costs. This is true for society as a whole, and specifically for employers when the concept is applied in the workplace. As with other human rights, privacy is not to be treated as an absolute value. However, a major problem with application of the concepts of reasonable expectations of privacy and consent is the fact that the analysis does not even get this far. If there is no expectation of privacy, or consent to privacy-invasive practices is found to exist, then a right of privacy does not exist at all. There is therefore no question of considering the employer's needs and interests. If there is no right of privacy, employers are simply free to act as they wish.
A preferable approach is to treat the issue as a question of balance. Employers may have their reasons for invading employee privacy, but these reasons should be tested against the impact on a recognised human right. What this comes down to is a proportionality analysis, the third theme which has emerged from the study of UK and Canadian approaches towards workplace privacy in the context of e-mail and internet monitoring. This is the requirement that the severity of an invasion of individual privacy is balanced against the justifications for and extent of the invasion in question, such that any interference with privacy rights must be "proportionate". To put it another way, whenever an employee privacy right is potentially being infringed, the employer should be required to justify its actions rather than being able to rely on express or implied terms of the contract of employment.\textsuperscript{508}

In the UK, proportionality is central to the HRA. As discussed in chapter two, the HRA is structured so that justifications for privacy invasive conduct are balanced against the right of privacy, and will only succeed in defeating the right if this is "necessary in a democratic society". This concept has been interpreted as being a proportionality test, (although, as already noted, if there is no reasonable expectation of privacy this stage is never reached). Proportionality is also very important to the DPA.\textsuperscript{509} As an alternative to consent in making data processing fair and lawful, the DPA contains a balancing test, in which prejudice to the data subject's rights and freedoms is balanced against the data controller's legitimate interests. As discussed further in chapter two, there is some concern about the weighting of this proportionality test, which appears to be in the data controller's favour and inconsistent with the requirements of the Directive. However, the DPA also contains a more general and overriding proportionality test, by requiring that data be processed only for specified and lawful purposes, and that such data should be adequate, relevant and not excessive. These provisions have been interpreted by the Information Commissioner in the Draft Code as requiring a proportionate approach in all cases of data processing within the employment relationship, such that all intrusions on employee privacy should be in proportion to the benefits to the employer, and the least intrusive method of achieving the employer's aims.

\textsuperscript{508} See Morris (2001) \textit{supra} note 175 in relation to the HRA and the \textit{Convention}.

\textsuperscript{509} See section 2.4.1 of chapter two.
should be used. Proportionality is also included in some of the Canadian privacy legislation. PIPEDA contains a requirement that personal information should be collected, used and disclosed only for purposes that a "reasonable person" would consider appropriate. As already noted, this appears to be a partial proportionality test. The purposes of information collection are scrutinised according to considerations of reasonableness, but this does not seem to include an assessment of the severity of the impact of the conduct in question on individual privacy – although recent comments by the PCC do suggest that the proportionality test may be interpreted more widely. Proportionality is also contained in the provincial privacy legislation in Saskatchewan, Newfoundland and British Columbia, where the nature and degree of individual privacy is that which is "reasonable" in the circumstances, with regard to the lawful interests of others – a test whereby the effect on individual privacy is balanced against the reasons for privacy-invasive conduct, (although it has already been noted that the definition of what is "reasonable" is unclear, and exceptions which include consent circumvent the proportionality test entirely). With specific reference to the workplace, some of the grievance arbitrations dealing with video surveillance of employees also adopt a proportionality approach. This test was used in Puretex, Thibodeau-Finch, St Mary's, and Re Brewer's Retail. In each case the approach was to balance the individual's right to privacy against the competing considerations of the employer's reasons for carrying out the surveillance in question.

Perhaps the best example of a proportionality analysis in relation to employer surveillance of employees in the workplace is the grievance arbitration case of Puretex. Although the employees in this case were fully aware of the installation of video surveillance cameras, and

510 See section 2.4.2 of chapter two.
511 See section 3.1.3 of chapter three.
512 Supra note 72.
513 See section 3.1.4 of chapter three.
514 See section 3.4.2 of chapter three.
515 Supra note 391.
516 Supra note 361.
517 Supra note 396.
518 Supra note 402.
519 Supra note 391. See also the discussion at section 3.4.2 of chapter three.
therefore under an empirical approach towards expectations of privacy would seemingly not have a privacy right at all, the arbitrator treated the issue as one of balancing competing interests. The effects on employee privacy and dignity were to be weighed against the employer’s justifications for the surveillance, which were based on efficiency. The arbitrator saw the full-time use of video surveillance for observation of work performance and employee conduct as "seriously offensive in human terms", such that only extremely compelling considerations of efficiency could justify the practice, but recognised that "changes in the quality and purpose of the surveillance may also lessen its 'inhuman' quality". The purposes of the surveillance and the way in which it was carried out were balanced against the impact on privacy – a classic proportionality test. The terms of the employment contract, and the employees’ factual expectations about privacy at work, were not relevant to the analysis.

Proportionality is a concept applied by the Supreme Court of Canada in Charter jurisprudence. In the case of *R v- Oakes*, the Court considered the test for deciding whether a limitation on rights under the Charter was reasonable and justified in a free and democratic society, which involves a proportionality analysis. Firstly, "the objective, which the measures responsible for a limit on a Charter right or freedom are designed to serve, must be 'of sufficient importance to warrant overriding a constitutionally protected right or freedom'". Secondly, the Court went on to consider the specific components of a proportionality test, which was divided into three aspects:

"First, the measures adopted must be carefully designed to achieve the objective in question. They must not be arbitrary, unfair or based on irrational considerations. In short, they must be rationally connected to the objective. Second, the means, even if rationally connected to

---

522 Although it should be noted that this was an interest arbitration, rather than one concerning the terms of the collective agreement itself. Arbitrator Ellis did note that this was not a question of whether the employer had a right under the management clause to install the cameras, and in fact assumed that it did have this legal right (*Ibid.* at 24), but the contractual position was not relevant as the arbitrator was deciding a dispute irrespective of contractual rights. However, for the purposes of this discussion, the approach taken in this case is put forward as the appropriate one even in cases where the contract of employment could otherwise be seen as deciding the issue.
524 *Ibid.* at 138 per Dickson CJ.
the objective in this first sense, should impair "as little as possible" the right or freedom in question... Third, there must be a proportionality between the effects of the measures which are responsible for limiting the Charter right or freedom, and the objective which has been identified as of "sufficient importance". 525

This involves consideration of the "ends" served by the infringement of Charter rights, namely the objective which the measures are designed to achieve, and also the "means" used to achieve this objective, effectively the way in which the ends are being pursued. In the context of workplace information privacy, this analysis can be used in formulating some basic principles which should be borne in mind when carrying out a proportionality test.

In relation to "ends", it is necessary to consider the specific interests of the employer which are being served by the privacy-invasive practice in question. This is more than simply confirming that the employer has a justification for its conduct – it is the strength of this justification which is important. The flaws of an approach which simply looks at the employer’s reasons for its conduct are illustrated by RIPA and the Lawful Business Practice Regulations in the UK. 526 These limit monitoring of employee communications to that carried out for a specific list of reasons. However, without any analysis of the importance of these reasons, invasive monitoring is "justified" so long as an employer can nominally bring itself within one of the relevant categories – so providing insufficient protection of employee rights. The outcome of any balancing test will depend on the extent of the impact on employee rights as well as the strength of the employer’s justifications, so it is not possible to generalise about the types of employer interests which might be given priority in applying a proportionality analysis. In the context of e-mail and internet monitoring, all of the reasons discussed in section 1.5 of chapter one could potentially be successful, depending on the circumstances of the case in question. However, it can be said that justifications based on protection of other human rights, or those based on the same interests as those protected by privacy such as autonomy, dignity and wellbeing, 527 are those most likely to be successful. For example, in relation to e-mail and internet monitoring, interceptions which are carried out to catch the perpetrator of sexual or racial harassment can be seen as upholding the

525 Ibid. at 139 per Dickson C.J.
526 See further section 2.3 of chapter two.
victims’ right to equality. This justification for infringements of privacy can therefore be given significant weight as it furthers another fundamental human right. It can also be argued that justifications based on purely economic considerations should be treated with some care. As discussed earlier in this chapter, one of the major concerns about a purely market-oriented approach towards the employment relationship is the desirability of allowing fundamental rights to be traded for economic gain. This argument applies equally to purely economic justifications of privacy-invasive practices. Again, there is a danger that a cost-benefit analysis will be allowed to dictate the levels of privacy protection, which does not afford appropriate respect for a recognised human right.528

In relation to “means”, it is necessary to analyse whether the employer could have behaved in a less intrusive manner. If an alternative approach towards furthering the employer’s interests would have had the same effect as the invasive practice in question, the employer’s conduct will not be justified even if the reasons for the conduct are particularly compelling. This involves consideration of both the method chosen to achieve the employer’s ends, and also the extent of the impact of the practice on employees as a whole. In the UK, the Information Commissioner’s Draft Code529 provides a good example of this aspect of a proportionality test. Two of the Draft Code’s overriding principles are that the method of achieving the employer’s aims with least impact on privacy should be chosen, and monitoring should be specifically targeted at achieving these aims.530 The Draft Code goes on to provide a number of examples of how these principles should be applied in practice. Telephone calls should only be monitored or recorded if an itemised call record is not sufficient for the employer’s purposes, e-mail monitoring of content should only be used if less intrusive monitoring could not achieve the same purposes, and similarly monitoring of internet use should only take place if restriction of access or recording of time spent on the internet would not accomplish the same aims.531 It is also emphasised that monitoring of all staff will not be justified if the purpose is to address a risk posed only by a few individuals.532

527 Craig (1999) supra note 16 at 163.
528 Ibid. at 164.
529 See further section 2.4.2 of chapter two.
530 Paragraph 6.1.
531 Paragraphs 6.3.1, 6.3.2 and 6.3.3.
532 Paragraph 6.1.
and monitoring should be targeted on the areas of highest risk. The Draft Code clearly shows how the "means" chosen by an employer can be tested in relation to monitoring of employees, the overriding principle being that the employer should only intrude on employee privacy to the extent truly necessary for the achievement of specific aims.

4.5 Conclusions

Privacy ought to be treated as a value which operates outside the employment contract, constraining the employer's ability to dictate terms and conditions of employment in light of the imbalance of power which is inherent in the employer/employee relationship. However, in practice the application of the ideas of reasonable expectation and consent, which are central to many definitions of privacy, equates to contracting-out of workplace privacy rights. This is coupled with a prevailing labour law approach which emphasises freedom of contract and employers' rights to set workplace terms and conditions. The overall effect is that privacy rights may be granted in the employment contract, in which case even an analysis based on freedom of contract will protect those rights, but otherwise their existence is left to the employer's discretion. When information privacy is put together with the employment relationship, the outcome is a mix which undeniably favours the employer. Indeed, this approach goes so far as to render the idea of workplace information privacy rights an empty concept. Proportionality is a preferable approach because it enables the law to fulfil the demands of industrial justice, while also recognising employer interests – but without giving those interests automatic priority over an undeniably important right in today's society.

533 Paragraph 6.3.
5 CONCLUSION

"Workers’ rights to privacy should be treated as a fundamental human rights issue." (International Labour Office) 534

"Employees have a fundamental, inherent right to privacy in the workplace." (Privacy Commissioner of Canada) 535

Privacy is a right which needs to be safeguarded in the modern world. This is particularly the case with information privacy, as is illustrated by the new legislation on this subject which is being introduced in both the UK and Canada. In the face of advances in technology, the ability to gather personal information about individuals is expanding all the time. This is as true in the workplace as it is elsewhere in society. In 1890, Warren and Brandeis noted that "numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’" 536 Computer technologies now have the capability to fulfil this prediction, and in light of the importance of the values served by privacy genuine legal controls are vital for protection of both employees and society as a whole. The issue of e-mail and internet monitoring provides a prime example of a recent technological development which potentially has a huge impact on individual privacy rights.

As has been shown in chapters two and three through an analysis of the law relating to monitoring of e-mail and internet use, both the UK and Canada give mixed messages about protection of information privacy in the workplace. In the UK, a new right of privacy has been introduced by various conflicting pieces of new legislation, leaving employers and employees alike unsure as to their rights and obligations. In Canada the law is a mixture of legislation and caselaw, much of which is not expressly directed at the employment context. Protection often depends on which province the employment in question is based in, and whether that employment is public or private, or federally or provincially regulated.

534 ILO (1993) supra note 1 at 77.
535 Supra note 72.
536 Warren & Brandeis (1890) supra note 5 at 195.
However, it has nevertheless been possible to identify some common themes which shed some light on how workplace information privacy rights tend to be regarded.

An important common theme is the way in which central privacy concepts, particularly the ideas of reasonable expectations of privacy and consent to privacy-invasive practices, interact with the dynamics of the employment relationship. As has been shown in chapter four, application of these concepts in the workplace results in contracting-out of the right of privacy. Indeed, in some cases it is not even a matter of contract, being left entirely to employer discretion. This means that the right to privacy fails to operate as an external limitation on the parties’ freedom of contract.

However, there is more going on here than simply a problem with translation of privacy concepts to the workplace setting. The issue goes deeper, showing a prevailing attitude towards the employment relationship which treats employee information privacy rights as a matter to be negotiated between the parties. Both caselaw and legislation take a deferential approach towards the employer’s management prerogative to control what goes on in the workplace – in the absence of express assurances of privacy, the employer’s interests hold sway. Concepts central to the definition of privacy, such as reasonable expectations, are used and interpreted in the workplace context so as to limit rather than enhance employee rights. Information privacy is therefore effectively treated as a right which is dependant on agreement between the parties to the employment contract – it may be obtained through negotiation, but otherwise rarely constrains the employer’s power. In contrast to the treatment of other human rights which may be of direct application in the workplace, and the more general trend in labour law for other external limitations to be placed on the parties’ ability to contract, information privacy is not seen a fundamentally important right such that the demands of industrial justice require interference with freedom of contract.

This outcome is puzzling. Why is information privacy not regarded as a constraint on negotiated terms of employment? It is clear that this right is somehow viewed differently from other rights and employment standards. However, the rationale behind the prevailing approach is certainly not articulated in the various court and arbitration decisions. Part of the
explanation must be the novelty of the issue. Information privacy is undeniably a new concept in the workplace, particularly in relation to use of computer technology. When faced with a new challenge to the freedom of contract analysis of the employment relationship, the courts simply take a while to catch up. Invasion of information privacy rights may also presently be seen as less intuitively “wrong”. In Canada at least, there is more recognition of the need to protect personal and territorial privacy rights, especially in the context of bodily searches and searches of desks, lockers and other private spaces. It is unlikely that an argument that employees had no expectation of privacy because they had been told to expect such searches would succeed in limiting privacy rights, and similarly there is likely to be more scepticism about “consent” to such practices.537 The idea of gathering “information” about workers is a much more intangible concept than that of subjecting workers to degrading physical searches. The loss of dignity involved in a personal or territorial search is more immediately obvious than that involved in invasions of information privacy, and therefore the relevant privacy rights are more readily recognised – although, as has been explored in section 1.2 of chapter one, invasions of information privacy can have an equally damaging effect on both dignity and other values. Both the UK and Canada have generally moved away from a strict freedom of contract analysis of the employment relationship, giving effect to external constraints on the bargain which can be reached between the parties, but when faced with these novel concepts the courts and legislators are falling back on a more traditional approach towards regulation of the workplace.

An additional reason why this approach is being taken becomes apparent when one considers the nature of the interference with management prerogative which is potentially involved when information privacy rights are enforced in the workplace. The protection of information privacy tends to result in direct interference with how the employer runs the workplace. This is more of a challenge to employer prerogative than is presented by other rights and employment standards. Taking the specific example of e-mail and internet

---

537 The general principles which have been developed in arbitral jurisprudence in relation to searches are that employee privacy is given priority unless there is a real and substantial suspicion of wrongdoing and the search is conducted reasonably (at least in the absence of a clear contractual right to search). See Brown & Beatty (1997) supra note 358 at 7-193; and see for example Lornex Mining Corporation Limited (1983), 14 L.A.C. (3d) 169 (Chertkow); Royal Oak Mines Inc (1992), 25 L.A.C. (4th) 26 (Bird); University Hospital (1981), 28 L.A.C. (2d) 294 (Picher).
monitoring, as outlined in section 1.5 of chapter one, employers potentially have a wide variety of justifications for this privacy-invasive practice. These justifications include quality control and supervision, enforcement of discipline, and protection of the employer's property and business. When employers are prevented from carrying out such monitoring, they are effectively being prevented from controlling their own workplace. Their ability to manage, supervise, and discipline is being constrained, and they are being told what they can and can't do with their own equipment on their own premises. Concern about this loss of management control seems to be behind much of the discussed legislation and caselaw which limits or denies workplace privacy rights — the grievance arbitration decisions which emphasise the fact that employees are using their employer's equipment on the employer's premises and should expect to be observed and/or supervised, the idea that employers should be able to control privacy expectations, and the approach of the Lawful Business Practice Regulations which ensures that employers' ability to monitor for business-related reasons remains unconstrained.

This is where information privacy can be seen as different from other rights and employment standards, which do not involve such a direct interference with management prerogative. For example, discrimination law limits the employer's ability to treat protected groups unequally, but the employer is still free to run the workplace as it sees fit so long as everyone is treated without discrimination. This therefore operates as a very narrowly targeted limitation on management control, in circumstances where an employer is unlikely to have a compelling justification for wanting to discriminate. Looking at the typical case where freedom of expression might be asserted in the workplace, namely that of whistleblowing by an employee, the right operates as a specific limitation on what an employer can prevent an employee from doing rather than a more general interference with working methods, supervision or discipline. Employment standards also tend to limit the employer only in very specific ways, affecting the terms of the contract between the parties. Typical examples in the law of the UK and Canada would be minimum notice periods, minimum wages, and limits on hours of work - all of which control an aspect of the terms and conditions of work, but do not interfere more widely with the running of the workplace. Health and safety standards may be seen as more of a limitation on management prerogative, but as these
constraints are designed to prevent actual physical injury, they are much more easily accepted than the somewhat intangible need for personal privacy.

Information privacy rights can therefore be seen as posing a new type of challenge to freedom of contract and the employer's prerogative to control the workplace. This helps to explain the reluctance of the law in both the UK and Canada to provide meaningful protection of employee information privacy rights, in contrast to other rights and standards. The law has come a certain way towards accepting external constraints on the employment contract in order to uphold specific values, but direct and pervasive interference with management and supervision in the employer's own workplace is a step too far.

The exceptions to this prevailing approach come from the specialist privacy commissioners - the Information Commissioner in the UK, and the PCC and the Ontario IPC in Canada. The Information Commissioner's Draft Code applies the general principles of the DPA to the question of workplace monitoring in a way which recognises fully the demands of employee information privacy, adopting a proportionality approach. Despite the limitations of the federal Privacy Act, the PCC has made recommendations about workplace e-mail and internet monitoring which emphasise the requirements of proportionality. The PCC has also interpreted PIPEDA as placing genuine limits on the ability of employers to carry out wholesale monitoring, emphasising the requirement for any monitoring to be "reasonable". The Ontario IPC has specifically considered the question of workplace computer monitoring, and recognises that employees can expect some degree of information privacy in the workplace. None of these commissioners takes the view that levels of workplace information privacy can be dictated by the employer or the employment contract. Unlike arbitrators and the courts, and legislators when faced with intense lobbying by employers, they are not constrained by attitudes towards the employment relationship which are based on freedom of contract. Instead, privacy principles contained in general legislation are applied to employment in a way which results in genuine protection of employee privacy rights. As has been expressed by one Provincial Privacy Commissioner, "...at the end of the day, what we are trying to do as privacy commissioners is to prevent, as much as possible, unnecessary surveillance of one another as human beings by governments, by corporations, or by our
fellow human beings. Without being limited by a traditional labour law approach, the information and privacy commissioners are able to recognise that this principle has equal force within the workplace as elsewhere in society. They are more familiar with the novel concept of information privacy, and less concerned about the amount of interference with management prerogative which is inherent in recognition of such rights.

The fundamental problem with the prevailing attitude is that in many cases it results in a complete denial of information privacy rights in the workplace. The possibility that employees might have legitimate privacy interests is not recognised at all. This is simply not sufficient when what is at stake is a human right, serving values which are vitally important to society. In chapter four, the concept of proportionality is advocated as an alternative approach towards workplace privacy rights. As emphasised by the various information and privacy commissioners in the UK and Canada, and adopted in some of the discussed legislation and caselaw, this enables the privacy rights of employees to be taken seriously while simultaneously recognising genuine employer interests. If concern remains about the extent of external interference with managerial prerogative, then this can be taken into account in the balancing process. However, a brief note of caution should be sounded here. If the dominant approach in the law is for freedom of contract and employer interests to be given priority, then there is a danger that this trend will continue where a proportionality test is being applied. It is important that information privacy rights are given appropriate weight in the balancing process – otherwise there is a risk that employer rights to control the workplace will unjustifiably be given more protection than employee privacy. The balancing test in the DPA which is heavily weighted in the data controller’s favour is an example of how a “proportionality” test may still unfairly advantage one party over another.

This failure to protect information privacy in the employment context is a particular problem because employees can be seen as a uniquely vulnerable group, deserving of additional rather than less privacy protection. The discussion in chapter four about theories of the

---

538 Flaherty (1999) supra note 312 at 225. David Flaherty was the Privacy Commissioner for British Columbia between 1993 and 1999.

539 See section 2.4.1 of chapter two.
employment relationship has already considered the imbalance of contractual power between employer and employee, and why this means that leaving employee rights to contractual negotiation can be seen as inappropriate. This vulnerability becomes even more marked when one considers the amount of time which may be spent at work by the modern employee, and the importance which work serves in most people’s lives. A job is often no longer a matter of “nine-to-five”, leaving ample time for private activities. An increasing long-hours culture, remote working, and working from home, all result in “work” impinging on “private” time. The Supreme Court of Canada has recognised that employees are a vulnerable group within society, and this vulnerability is not limited to the employment contract but relates to “virtually all facets of the employment relationship”. Indeed, in some ways the employment relationship can be seen as analogous to the relationship between the state and its citizens. However, approaches towards information privacy which view workplace rights purely as a matter of private ordering are treating employees as a less rather than more vulnerable group than others within society.

The employment relationship also involves a lot of the fundamental interests which are protected by the right to privacy, so making the right particularly important in the workplace. If individuals spend the majority of their time at work, the democratic function served by the ability to develop ideas and exercise personal autonomy will certainly be impaired if there is no privacy in the workplace. It is also clear that denial of privacy at work can have a particularly damaging effect on dignity and personal wellbeing. The employment relationship itself inevitably involves workers in giving up a degree of personal autonomy, and the inherent imbalance of power between the parties allows scope for abuse and excessive control by employers. Limitation of information privacy rights in such a setting is uniquely damaging to individual dignity, as the modern employee has no escape:

“Under the old school of scientific management, the alienated worker did what he or she was told, got paid, and went home. The work may have been boring, the wages low, but at least everyone knew where he or she stood. Today the transaction is not as honest. While we still trade our labour, most modern work requires us to give away a slice of our private lives, Workers of the past were just overworked; today many workers are overworked and

540 Wallace v United Grain Growers supra note 353 at 32.
541 See further section 1.3 of chapter one.
overmanaged. The exhaustion that paints the faces of workers at the end of the day may not be physical but emotional, because work demands more of the self than accurate and efficient performance of the task at hand.\textsuperscript{542}

When the unique vulnerability of employees is coupled with the fact that the values protected by privacy are particularly in danger in the employment relationship, the importance of information privacy rights being afforded a high degree of protection in the workplace is clear. However, as has been shown by the comparative study of UK and Canadian law, in practice the opposite is the case.

It is to be hoped that over time information privacy in the workplace will obtain increased recognition, potentially aided by advice and pressure from the information and privacy commissioners. It is particularly crucial that this change in attitude takes place in relation to the challenges posed to privacy by rapid advances in technology. With specific reference to e-mail and internet monitoring by employers, the scope does exist for a more employee-protective approach to be developed. In Canada, the groundwork is there with some of the Charter jurisprudence, and those arbitrations concerning workplace video surveillance which adopt a proportionality analysis. In the UK, the contradictory approaches in the new legislation could be resolved in favour of information privacy rights rather than employer interests. However, this will require a move away from current attitudes towards information privacy in employment, and a willingness to recognise that the wider claims of society may justify interference with employer control over the running of the workplace.

The International Labour Office has expressed the view that "workers’ rights to privacy should be treated as a fundamental human rights issue."\textsuperscript{543} As has been demonstrated by this study, at present neither the UK nor Canada gives workplace information privacy rights the protection required to make this statement reality.


\textsuperscript{543} ILO (1993) \textit{supra} note 1 at 77.
BIBLOGRAPHY

Books and Articles

ADAMS (1978) – Grievance Arbitration of Discharge Cases (Kingston, Ontario: Industrial Relations Centre, Queen’s University).


AUSTIN (2001) – “Privacy and the Question of Technology” (on file with the author).


BARNACLE (1991) – Arbitration of Discharge Grievances in Ontario – Outcomes and Reinstatement Experiences (Kingston, Ontario: Industrial Relations Centre, Queen’s University).


Studies and Reports


PRIVACY FOUNDATION (2001) – The Extent of Systematic Monitoring of Employee E-mail and Internet use (Privacy Foundation, Workplace Surveillance project).