J. INDIVIDUAL EMPLOYMENT RIGHTS, Vol. 11(4) 291-310, 2004-2005

BALANCING EMPLOYEE AND EMPLOYER RIGHTS: AN INTERNATIONAL COMPARISON OF E-MAIL PRIVACY IN THE WORKPLACE

ANDRÉ M. EVERETT
University of Otago

YIM-YU WONG
San Francisco State University

JOHN PAYNTER
University of Auckland

ABSTRACT

The rising prevalence of e-mail as a means of both business and personal communication is accompanied by multiple possibilities for negative effects on organizations whose employees utilize e-mail and Internet services while at work. These include not only transmission of confidential business information but also simple waste of time, decreasing employee productivity. To limit such potential abuse, employers in many countries have tended toward monitoring of employee Internet activities in the workplace. With a lack of clear guidance on appropriate mechanisms for such monitoring and surveillance, issues of personal privacy have arisen. Our article examines some of the underlying issues linking e-mail/Internet monitoring and employee privacy in the workplace from an international perspective, including examples of relevant legislation from selected countries.

Electronic mail (e-mail) is a powerful, widely-used communication tool, facilitated and enriched by rapid growth in use of the Internet. Since the Internet is international, people can communicate and exchange data and information with each other around the world. However, because it is international, technologically complex, and dynamic, legislation and enforcement governing activities on the Internet are underdeveloped in nearly all countries. As a result, privacy

problems may arise, since individuals and organizations are able to easily collect personal information about others. In particular, e-mail can provide long-term records of personal information including contacts, beliefs, transactions, intentions, work activities, and more. Companies are increasingly troubled by the abuse of e-mail and inappropriate use of the Internet at work [1]. Among individuals, there is a lack of awareness about how extensively personal information has been collected on the Internet and with whom this information is shared. Most people do not realize the consequences and potential for misuse if a company or person obtains their personal information. This situation has led to a growing privacy rights movement, resulting in legislation affecting the privacy of electronic communications and personal information in various ways in many countries.

This article focuses on the issue of monitoring and surveillance of employee e-mail, considered from several national legislative perspectives. Privacy issues related to the use of computer technology to monitor the activity and performance of employees in the workplace are not new, and are widely discussed. Privacy is the condition of not having undocumented personal knowledge about oneself possessed by others; the concern in this article is to examine the question of whether monitoring employees' e-mail messages in the workplace is an invasion of personal privacy or a prudent protection for business security.

Our methodology applies a critical perspective to the literature and legislation in selected countries, employing an extensive academic literature review (only a small portion of which is mentioned here), examination of legislation published in several languages, dissection of practitioner reports of extant policies and their effects, comparison of policy construction recommendations by information systems and legal consultants, discussion with an informal sample of information system managers, comparative analysis, and argumentation. We also relied and drew extensively on our collective expertise in the information technology and international management fields, where we have been actively researching and reflecting on related topics for the past twenty years. One of the motivators underlying this study was our eye-opening experience in assisting in the development of e-mail policies in our own organizations.

Whose rights are more important—the individual's right to privacy or the company's security? Do we need to claim a balance of rights between employers and employees, and where should this balance be struck? Is there any gray area that can be potentially dangerous to either party? These issues remain controversial. In addition, there are few authoritative answers regarding how existing laws apply to e-mail. Professional opinions on the implications of various pieces of legislation that are coming into effect are even scarcer.

E-MAIL PRIVACY

The definition of privacy varies widely across contexts and environments in different countries. In general terms, privacy protection is frequently seen

as "a way of drawing the line at how far society can intrude into a person's affairs" [2]. Bloustein regarded invasion of individual privacy as "demeaning to individuality, . . . an affront to personal dignity" [3, p. 973]. To Kovatch, privacy means "freedom from unwarranted and unreasonable intrusions into activities that society recognizes as belonging to the realm of individual autonomy" [4, p. 4].

The Australian Privacy Charter provides that "a free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organisations to intrude on that autonomy. Privacy is a value which underpins human dignity and other key values such as freedom of association and freedom of speech. . . . Privacy is a basic human right and the reasonable expectation of every person" [5]. Privacy has also been defined as "the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behavior to others" [6, p. 7].

Many countries interpret privacy issues in terms of the management of personal information and data protection. The power of new technology and the Internet in particular allow data and information to be collected, matched, combined, manipulated, and transmitted in a nanosecond [7]. In terms of e-mail privacy, the issues become even more complex and difficult to define. "What protected us, to an extent, in the past, was a wall of paper. . . . Now electronic communication allows that wall to be penetrated very easily" [Donald Harris, quoted in 7, p. 33]. The dawning virtual world has engendered entirely new interpretations of and limitations on privacy, dramatically diminishing the shields that differentiated one's private from one's public persona [8]. Many companies have found themselves embroiled in controversy on the rights of employers to monitor employee e-mails. To what extent does an employee have a right to privacy in the workplace? The lack of a standard single definition of personal privacy should not imply that the issue lacks importance.

E-mail is a powerful tool for business communication through the Internet. A Pitney Bowes survey conducted in 2001 found that for the first time, e-mail had surpassed all other forms of communication in U.S. and Canadian workplaces, with 96 percent of workers reporting its use every day or several days per week [9]. The 2004 Digital Future Report indicated that of U.S. workers who have Internet access at work, 85.9 percent used it for work-related e-mail and 63.5 percent for personal e-mail; two-thirds indicated having access at work made them more productive (31.7 percent much more, 34.1 percent somewhat more, 27.9 percent neither more nor less, 5.3 percent somewhat less, and 0.9 percent much less productive) [10]. (However, disparate measures will result in widely different readings; for example, a 2003 study found that 45 percent of workers in the United States were without e-mail, although this number would halve over the next four years [11]). The 63.5 percent personal e-mail use figure may sound alarming, but this should be balanced against the December 2002 survey by the Center for

E-Service, where employees with Internet access at both home and work spent 3.7 hours per week on personal Internet activities at work—and 5.9 hours at home on Internet-related work activities [12].

Our intention in this article is to examine e-mail privacy, rather than whether or not employers benefit from employees' private use of Internet facilities at work. We do not advocate eliminating personal e-mail access at work, given the presence of numerous pros and cons that can be balanced through judicious creation and application of organizational policies. On the positive side, personal e-mails are similar to personal telephone calls, used both for convenience and in emergencies. Banning employees from making personal phone calls, e.g., to make a doctor's appointment when the only chance to do so is during office hours, would be considered unreasonable and demotivational by many employees. A significant portion of households with children has dual-income earners who must check on their children after school hours. Employees who do not have Internet access at home may consider this an added benefit; others may remain on site during lunch hours to utilize the Internet, rather than leaving to run errands; both perspectives can lead to greater overall productivity and loyalty. Allowing some personal e-mails can also be construed as similar to allowing personal telephone calls, within reasonable limits.

On the negative side, efficiency and productivity might be lowered due to excess time spent on personal e-mailing. Companies can be held liable for unlawful materials received through and stored on employer-owned computers. The company's responsibility to establish e-mail policies and provide guidelines is discussed later. Instead of banning personal e-mails, companies could allow employees to use their break times for this purpose. To discourage spending work time on personal matters, companies can set aside computers in break rooms or lounges for personal e-mailing or general Web surfing while establishing a policy of no personal e-mails on work computers. Employees may also be allowed to bring their own laptop computers for use during breaks.

With the resulting widespread availability of access to the Internet and e-mail in the workplace, there is no doubt that this access could be abused. However, although it is difficult to find quantitative evidence of the scale of the abuse, employers may monitor their employees' work activities to prevent such abuse in the use of business services and equipment. Therefore, an employee's expectation of a certain level of privacy is often in conflict with the employer's need to maintain a productive level of operation [13].

E-MAIL PRIVACY RIGHTS?

The questions of "Whose rights are more important—employees' privacy or the company's security?" and "To what extent can an employer justifiably infringe an employee's right to privacy?" have been raised. Banisar stated that "[e]mployers' collection of personal information and use of surveillance

technology is often justified on the grounds of health and safety, customer relations or legal obligation. However, in many cases workplace monitoring can seriously compromise the privacy and dignity of employees. Surveillance techniques can be used to harass, discriminate and to create unhealthy dynamics in the workplace" [2].

E-mail messages sent on a company-owned computer network should be regarded as business communications within the organization [14]. U.S. "courts have affirmed that employees have a limited right to be protected from unreasonable intrusion into their private affairs. At the same time, the legal requirement that employers maintain a safe, harassment-free and drug-free workplace often requires some level of employee monitoring" [15, p. 31]. There are even multiple benefits of workplace monitoring that can be gained by both employer and employees: It can help improve the quality of a company's goods and services provided to customers; it can improve efficiency and profitability of the business that may lead to higher pay for those employees who are doing their jobs well; and it can improve the work practices of the employees [14].

Moreover, some developers of monitoring software believe that the issues of workforce harassment, sex discrimination, and other sensitive issues may make it the employer's responsibility to monitor and search the e-mail of employees or their use of the Internet in general [16]. Any company not doing this could be liable for breaches of the law with respect to defamation, obscene materials, employee harassment, or other improper activities if the company could have stopped it.

Conversely, in a classic treatise on workers' right to privacy published in 1890, Warren and Brandeis argued that employers have certain rights with respect to their employees, but there is no general and absolute right to monitor and control employees [17]. Although there are various benefits a business can gain from workplace monitoring, there are potentially unacceptable consequences that may occur due to workplace surveillance. Examples include harm related to employees' well-being and infringement of employees' rights to privacy. Evidence supports the notion that computer-monitored (including e-mail monitored) employees suffer stress, morale problems, and ill health to a higher degree than other employees not under surveillance [15].

Because all employers are purchasing the time and labor of their employees, conversations or e-mail messages between employees and clients may be regarded as the employer's business, but employers should not have the right to store and review their employees' personal conversations with others even though they are using the company's equipment to e-mail [14]. The fact that they are continually having conversations might be overloading the equipment or impeding their own work performance and the work of other employees. This raises the question, If there are problems such as overloading of the system or inadequate work levels, how will the employer know these problems are caused by the employees' misuse of e-mail services for personal purposes unless they monitor it?

Given the potential conflict between an employee's right to privacy and the rights of the employer to monitor its workplace, it is important to balance the rights of individuals against those of the community. There should be "a fundamental moral obligation to respect the individual's right to privacy, and the legitimate requirements of, for example, employers to monitor the performance of their employees, and law enforcement agencies to monitor the communications and financial transactions of organized crime" [14, p. 203]. Employers must tread a fine line between invasion of privacy (by digging into an employee's private matters) and risking harassment lawsuits (should an employee send offensive messages) [15].

In one case, a company was sued by some of its employees because the company's e-mail policy was "impossible to locate" on the company's intranet and it was difficult to understand—even though these employees had abused the e-mail system, i.e., forwarded sexually explicit e-mails to co-workers. In other words, the difficulty in locating and understanding the company's e-mail policy led the employees to believe that their personal e-mails were personal property and should not have been monitored by the company. Even though the court's decision held that the employees' view was not reasonable, it nevertheless alerted employers to the importance of ensuring that their e-mail policy is known to employees [18].

The resolution of these issues lies somewhere in the middle. Toten argued that the best compromise would be limiting private conversations and justifying short-term monitoring with the consent of employees [19]. Waltemath suggested that a restriction could be placed on the length of e-mail messages, or if necessary, the productivity and performance of the employees in question could be investigated [20]. Magney claimed that "employing people does not confer the right to monitor their private conversations, whether those conversations are in person or via email" [14, p. 204]. Monitoring e-mail privacy becomes an issue of balancing the rights of individuals against the needs of the community [21].

POLICIES AND PENALTIES

The most common suggestion is that organizations establish a clearly written privacy policy dealing with the use of e-mail and the Internet, while safeguarding employees' privacy [15, 19, 20]. In a 1987 decision by the U.S. Supreme Court regarding determination of when a search has violated an employee's privacy, three key considerations were identified: "First, does the employee have a reasonable expectation of privacy in the thing to be searched? Second, does the employer have a reasonable, work-related need or suspicion to search? Finally, the scope of the search must not exceed what is necessary to investigate the employer's need or suspicion" [4, p. 6].

When an employer communicates that policy to employees and applies it consistently, and employees know exactly what to expect, the likelihood of legal problems declines. The first step is to communicate with every employee about the policies that are developed, preferably obtaining their signatures to indicate their awareness and acceptance of these policies [16, 22]. Otherwise, employees will sense that employers are intrusive in the long run. It has been suggested that the "best policy . . . destroys the employee's reasonable expectation of privacy. It should make clear that everything done on the computer belongs to the company" [7, p. 34]. Communicating the privacy policy to all employees will "prevent the employees from being embarrassed at best and protect employers from legal liability at worst" [20, p. 114].

For monitoring to be effective, employers must show that it is routine, an ordinary aspect of business, and that there is a business purpose for intercepting and monitoring employees' electronic communications [23]. It may even be claimed that it would be unreasonable for an employer to not monitor such activities, given the potential dangers to the business as well as the actual costs and lost productivity. The policy should be strongly worded and comprehensive. It should stress that surveillance of any type can be conducted, unless the company chooses to limit the means of monitoring, so as to reduce any expectation of privacy. The policy must be circulated widely and frequently. In some states, e.g., Connecticut and Delaware, employers are required to provide employees with periodic notification of their monitoring activities. Essentially, the spirit is that employers have the right to inspect any employer-provided computer used by any employee at any time by any means [18].

However, one survey found that one-third of the responding companies had no such policy [7]. This question was indirectly addressed in the late-2002 UCLA survey, where more than one-quarter (26.9%) of employees said their Internet and e-mail activity at work was not monitored at all, and an additional one-quarter (28.1%) were unaware of any monitoring [24].

Typical key areas that an e-mail and Internet use policy can cover include:

Right to Monitor

"Email monitoring in organizations may be viewed by employers as a necessity, as well as as a right" [23, p. 49]. It is deemed obvious that employees have the right to protect their own privacy, and employers have the prerogative to preserve workplace efficiency and minimize risks of criminal activity. "What is less obvious is the extent to which an employer can justifiably infringe an employee's right to privacy" [21, p. 258]. The employer should develop a policy that makes it clear to the employees how the organization monitors and audits them and that it will retain the right to monitor and if necessary access any employee's e-mail messages, both sent from and received in the office, as well as any Internet use occurring from and files held on any company computers, as long as this can be

shown to be necessary and appropriate for legitimate business reasons [20]. As owner of the equipment and resources, employers can assume the right to monitor e-mails [23]. The range of available options begins with complete monitoring and extends to hands-off or no policy at all [25].

No Expectation of Privacy

In general, employees should have no reason to expect privacy when using employer-provided and owned technology [18]. There is no constitutionally guaranteed right to privacy in the United States, but the Supreme Court identified the existence of "zones of privacy" arising from other points in the Constitution [4, p. 4]. Employees' perceptions of their employer's e-mail policies can be affected by the technology factor, management policies, employee experience, management style, and social effects (e-mail creates the perception of privacy through social norms, mutual self-disclosure, and development of interpersonal ties) [25]. Employees should be informed that any e-mail sent on a company-provided computer is regarded as a public communication in the company even if the contents concern personal matters [21].

It is considered good practice to let employees know that the e-mail and Internet information generated in the company is considered business information, and any electronic communications in the office are the employer's property; it is therefore unreasonable to consider e-mail as personally private or confidential, regardless of whether it is business-related or personal [19]. Employees should not assume that e-mail messages or a history of the Web sites they have accessed cannot be retrieved after they have been deleted [20]. In public offices, the government's need to ensure efficient operation of the workplace may outweigh an employee's expectation of privacy, even if the privacy expectation is reasonable. The public sector employee's legitimate expectations are therefore diminished [23].

Personal Use

Employers should state explicitly that they have the right to insist that equipment and assets in the company (including the Internet and other computer equipment) are not to be used for anything apart from legitimate work-related purposes [21]. Employees should understand that any use of company computers for personal matters is not acceptable, including checking personal e-mails via the employer's Internet access [18]. Taking a more accommodating route, should the employer decide to permit personal use of e-mail and/or the Internet, employees should recognize that they must "act responsibly, appropriately and professionally before, during and after normal business hours" and that their use "must not be excessive and must not distract from organizational objectives" [20, p. 114]. Findings from studies of Internet usage at work indicate that in practice many employers tolerate (if not always condone) personal use of computers and network connections.

Prohibited Uses

The policy must state clearly what activities are prohibited in the workplace in relation to the use of e-mail and the Internet. For example, employees should be prohibited from using e-mail that is offensive or negatively affects the employer's reputation and/or employees' job performance [15]. To prevent intentional or unintentional damage to the employer's computer systems and network, restrictions should be placed on the types of file attachments allowed, such as excluding executables (program files that can be run, or "executed," typically bearing .exe file extensions) and movies (which may be excessively large in size, slowing the network, and have content that cannot be filtered or censored by available technologies) [26].

Discipline

Organizations have enacted substantial penalties for misuse of e-mail at work, including reprimands, suspensions, demotions, and terminations [18]. *The New York Times*, Xerox Corp., and First Union Bank have reportedly fired employees after determining "inappropriate" use of company-provided Internet access [7, p. 33]. In 2002, Hewlett-Packard UK found "a nasty surprise" on the company's e-mail server and suspended 150 employees, firing two for "viewing and sharing unauthorized and inappropriate material" as a result [27, p. 44]. At Lloyds TSB bank, the head of information technology security and risk said that the company issues a complete ban on all personal e-mail use by its 80,000 staff in 27 countries. He emphasized that he makes sure that "my staff know the rules"; they know that he monitors, checks, and investigates, and that if anyone breaks the rules, he will fire that staff member [27, p. 44].

CCH Incorporated, a legal firm claiming to be "a leading provider of employment law information and e-learning for human resource professionals," advises that the policy must state clearly to the employees "that anyone violating the rule against inappropriate use [of e-mail and the Internet] may be disciplined. Discipline may include oral or written warning, reprimands, demotion, suspension, probation or discharge" [28]. Further, "If the person who violates the policy is a manager or supervisor, a more severe penalty may be necessary" [28]. In a survey conducted by *CIO Magazine*, the vast majority of responding chief information officers said that abuse of e-mail in their firms would result in firing the offending employee—90 percent for sexual harassment, 84 percent for sending porn to co-workers, and 80 percent for compromising trade secrets [1].

Balanced Expectations

Other than the responsibility of employers for developing a clear policy on the use of e-mail and the Internet in the workplace, employers should also stress that employees have the responsibility of understanding that they should never input or

retain any personal information in the corporate system unless they do not mind employer access to it [7]. Everyone needs to protect him/herself in advance, as it is a fact that it may be necessary for employers to gain access to employees' private e-mails and files in some circumstances. This knowledge protects the interests of both the employees and the employer. Three questions have been suggested to determine whether an intrusion into someone's e-mail file is justified:

1. "Did the person have a reasonable expectation that his mail would be private? If you explicitly tell your employees that their e-mail will be monitored, then they can have no illusions of privacy.
2. Was the intrusion for a legitimate purpose, such as to monitor compliance with company policies or an investigation into alleged misconduct?
3. How far did the intrusion go? Did it go only as far as needed for the purpose?" [29, p. 66].

In practice, there must be a balance between an individual's privacy and the company's needs. "The first step would be to determine the severity of the problem and make sure there are legal grounds to investigate the problem. If you concluded the problem was intentional and severe, you'd want to handle it very tactfully and do it on a personal level" [22, p. 43]. Employers should educate existing and potential employees on the privacy issues in the workplace and should also treat them fairly at the same time [26]. While it may be necessary to monitor employees, such "monitoring creates increased stress, and often makes employees feel demeaned" [4, p. 5]. Establishing a positive relationship between employer and employees and maintaining a good working environment should help to minimize conflicts.

LEGISLATION

In 1997, the International Labor Office developed the "Code of Practice on the Protection of Workers' Personal Data," which safeguards employees' personal data and fundamental right to privacy. Banisar noted that "the code does not form international law and is not of binding effect. It was intended to be used in the development of legislation, regulations, collective agreements, work rules, policies and practical measures" [2].

Many countries have established laws protecting the collection and distribution of personal data; however, there are relatively fewer legal controls on workplace surveillance. Legislation differs across countries; research has shown that there is a significant association between the local culture and both interpretations of personal privacy and the regulations created to protect it [30]. The extent of the privacy to which employees are entitled in the workplace and how that privacy should be protected are not clearly and consistently specified. Legislation has recently been introduced in various countries that would prevent employers from secretly monitoring the communications and computer use of their employees.

Table 1. Summary of Country/Region Approaches to E-mail Privacy

Country/Region	Legislative level	Specific limitations on e-mail monitoring
Australia	National, some regional (state)	Incomplete but tending toward universal limits
Canada	National, some regional (province)	Incomplete but tending toward U.S. norms
China	National	No known specific limitations; focus is on permitting rather than on limiting monitoring
Czech Republic	National	Universal (limiting access by anyone)
European Union	Supranational, national, regional, and local	Cross-border data flows (rather than domestic access)
New Zealand	National	Universal but oblique (limiting access by anyone)
United Kingdom	National	Governmental; some corporate limits
United States	National, regional (state)	Governmental and corporate, complicated by interaction of diverse statutes

Examples of legislation introduced in selected countries/regions follows, with a summary provided in Table 1. The approaches taken range from acknowledged widespread monitoring without recognized employee rights, through a mixture of prohibitions and permissions, to a generalized protection of personal information that encompasses (and sometimes specifically incorporates) e-mail.

In **Australia**, the *Privacy Act 1988* and the *Privacy Amendment (Private Sector) Act 2000* require organizations in the private sector to follow certain guidelines in collecting, holding, using, disclosing, and transferring personal information; they do not, however, address employee privacy rights in the workplace [31]. One Australian court ruling in 2000 held that a union representative employee was unlawfully fired when she used the employer's e-mail system to send union-related materials to union members during her working hours; the dismissal was deemed unfair because communicating with the union members was part of her duties as a union delegate [19]. At the time of this writing, the Australian government had called for public submissions as part of a review of the *Privacy Act*, closing in mid-2005 [32]. Each state also

enacts laws governing such matters; New South Wales is in the process of extending its Workplace Video Surveillance Act 1998 to include e-mail surveillance of employees. The proposed extensions include a prohibition on e-mail monitoring without either a court order or a notice warning the computer user at the time the system is turned on [33].

In **Canada**, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) was phased in between 2001 and 2004, and "now covers all personal information of customers that is collected, used, or disclosed in the course of commercial activities by private sector organizations, except in provinces that have enacted legislation deemed to be substantially similar to the federal law" [34]. PIPEDA gives individuals the right to control how personal information (including e-mail addresses) is used; however, there are no specific provisions about employer monitoring of e-mails, or any mention of e-mail use in the workplace. Cautions regarding how individuals can protect themselves while using e-mail are provided by the Office of the Privacy Commissioner of Canada, but these are generic and not related to employer/employee issues. To date, no decisions by the privacy commissioner have been identified that dealt with use or content of e-mails, although several have focused on illegal revelation or collection of e-mail addresses [35]. Canada's rules on electronic communication are similar to those in the United States, including those that define an employer's reading of an e-mail message stored on one of its computers as not "intercepting" that message [36, p. 249]. It is not yet clear from either legislation or court interpretations whether the employee or the employer "owns" any e-mail sent by an employee at work [36, p. 249].

China represents a contrast with the remaining countries examined here; it is the only so-called "developing" country, and is well-known for distinguishing itself by adopting a uniquely Chinese approach to everything. This traditionally includes granting rights only reluctantly while maintaining governmental control, particularly at the central level, over as many aspects of civil life as possible. Consequently, we could identify no laws providing employees with protection from surveillance by their employers. The basic assumption of much of the populace is that monitoring is pervasive, whether at work or elsewhere, and that the boundary between public and private is both more fluid and closer to the individual than in Western societies. Nonetheless, Internet use in China is booming; with 94 million users at the end of 2004 (45% of whom have broadband access) [37], it attained second place by passing Japan in early 2002 [38]. Forty-one percent of those accessing the Internet do so at work, with e-mail being the most popular service, used by 85.6 percent, followed by search engines at 65.0 percent [37]. It is our experience that personal e-mail access on work computers is a widely accepted norm, but that employees are universally aware that their e-mail is almost certainly being monitored, if not by their employer then by the government, both via intelligent automated filters and human monitors. The e-mail senders persevere under these conditions, given that they match those found for

access from home or any other location, with official monitoring of Internet cafés and other public access venues the rule. Although there is universal awareness of this monitoring, a lively underground does exist, with arrests, prosecutions, and jailings of official policy violators frequently reported in the media. The situation in China is, overall, not comparable to that in the other countries included here.

The **Czech Republic** is one of the more advanced countries in Central and Eastern Europe, particularly in terms of Internet use, with 35 percent of the population accessing the Internet in 2004 [39]. There are no laws specifically governing electronic mail, but authors of e-mails (regardless of whether they are employees or not) have been afforded the protection of the Declaration of Human Rights and Freedoms (article 13) through the Constitutional Court's Opinion No. 536/2000, which states that secrecy of any transferred message (including telephone, fax, e-mail, postal, and others) must be guaranteed and protected as an aspect of individual integrity. Some employers have included in their employment contracts a clause whereby employees abandon this right, but this contradicts the notion contained in the Declaration of Human Rights and Freedoms that people cannot give up such rights, even voluntarily [40]. Employers accessing their workers' e-mails may face prosecution under paragraph 243 of the Czech Criminal Code on the inviolability of letters, which takes into account all messages, transferred by all means, that are intended for a given recipient. In that context, an addressed message may be read only by the intended recipient. Employers should be able to control their workers' Internet usage by examining volume of transferred data, rather than actual e-mail or network addresses [40]. As a member of the European Union, the Czech Republic is obliged to follow the rulings of European courts as well.

In the **European Union**, the *European Data Protection Directive 1995* "strongly limits the amount of personal data (social security numbers, employee ages, addresses, telephone numbers, and other basic information) that can be exported from an EU country to another country that does not meet stringent security standards for protecting this data during its transmission (electronic or otherwise)" [7, p. 34]. No specific rules affecting employer rights to monitor employee use of e-mail could be identified in a search of the European Union legal database [41]; the primary concern indicated in relevant documents was control of spam and unwanted or illegal content sent by e-mail. A proposed Decision of the European Parliament and of the Council addressing "safer use of the Internet and new online technologies" did not even mention employers or workers/workplaces [42, p. 3].

In **New Zealand**, the *Bill of Rights Act 1990* states, "Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise" [43, Section 21]. The *Human Rights Act 1993* prohibits discrimination. It encompasses rights including respect of privacy and freedom of expression. The accepted interpretation is that this includes e-mail messages, with the consequence that employers should not monitor the e-mail of

their employees [44]. The Privacy Act 1993 regulates "(i) The collection, use and disclosure, by public and private sector agencies, of information relating to individuals; and (ii) Access by each individual to information relating to that individual and held by public and private sector agencies" [45]. The Privacy Act applies directly to "personal information," which is any information processed either automatically or manually about an identifiable individual; as such, its intention is similar to the European Union's Data Protection Directive, but the broader nature of the Privacy Act (in combination with the aforementioned Bill of Rights and Human Rights acts) allows it to be applied in an oblique fashion as a general deterrent to monitoring. Additionally, personal grievance cases have been brought under the Employment Contracts Act 1991 [46] and the Employment Relations Act 2000 [47] regarding dismissal due to misuse of e-mail, but these cases resulted from complaints rather than from premeditated monitoring, and privacy was not the focal issue.

In the **United Kingdom**, the Regulation of Investigatory Powers (RIP) Act was enacted in July 2000. This act allows "police, MI5 and other even more clandestine law enforcing authorities to demand decryption keys to read the most confidential of confidential e-mails to/from/within our companies" [48, p. 18]. The Defamation Act 1996 [49] "makes it an offense in the U.K. to disseminate defamatory statements, including any via e-mail" [29, p. 66]. Also, although the Regulation of Investigatory Powers Act allows only limited monitoring of company e-mail, the Human Rights Act prevents employers from monitoring without reasonable suspicion. Such suspicion can be justified by an observed decrease in efficiency or a complaint filed by a fellow worker [27].

Under **United States** law, the documents and images that employees generate at the office belong to the business owner [7]. Employees have less bargaining power, in that they can either resign or give up all rights and expectations to privacy and freedom from invasion in the office. On the other hand, the legal principle is that the exposure of private facts can lead to litigation [7]. Kovatch discussed privacy rights in the work place [4] and Scott reviewed employee e-mail privacy [50], both from the legal point of view. The earliest court case known to specifically involve e-mail dates from California in 1991; two employees dismissed for violating a no-personal e-mails policy with awareness that e-mails were monitored by a supervisor were ruled to have no reasonable expectation of their e-mails being private [51]. Indeed, for employees in the United States, policies are considerably more relevant and important than laws in this context [52].

Some examples of particular U.S. cases reported in the media are enlightening in that they demonstrate the extent to which the law engages with e-mail privacy issues and how statutes from widely divergent domains can interact. In one instance, an employee attached the line "Have a Blessed Day" on every outgoing e-mail, and claimed that the request from her employer to remove this line violated her religious freedom [18, p. 5]. In another example, an employee used

"the truth shall set you free, but first it will piss you off" at the end of every outgoing e-mail and claimed that it was a violation of her First Amendment rights when her supervisor requested she drop the second part of the sentence [18, p. 5]. Both were required to drop or modify their use of these phrases by a court [18]. In a case where an employee was found observing child pornography online by the employer, who happened to be a public official, the employee sued the employer, claiming that while the employer has the right to monitor workplace misconduct, the employer has no right to investigate criminal misconduct. The court held that the public employer has the right to investigate workplace misconduct that happens to be illegal [18].

Public sector employees in the United States are protected by the Fourth Amendment to the U.S. Constitution, which safeguards personal privacy [4, 50]. However, this protection does not apply to employees in the private sector [50], whose privacy is regulated by a mixture of "federal and state statutes, common-law tort theories, and the public policy exception to the employment-at-will doctrine" [4, p. 5]. The minutiae of legalistic definitions sometimes catch people unawares, or can be utilized in unintended ways; for example, a 2004 ruling by the U.S. First Circuit Court of Appeals (going against the federal government) found that Internet service providers can access any aspect of an e-mail stored on their systems (in RAM or on a hard drive), because the messages are not being intercepted in transit; stored messages are governed by the 1968 Stored Communications Act, instead of the 1968 Wiretap Act or 1986 Electronic Communications Privacy Act [53]. A key point arising from this case is that e-mail is treated differently from popular expectations and from other forms of communication, resulting in the introduction in the U.S. Congress of two remedial resolutions on July 22, 2004, the E-mail Privacy Act 2004 (H.R. 4956) and the e-mail Privacy Protection Act of 2004 (H.R. 4977) [54].

When criminal investigations are involved, a company's e-mail files may be made public. This occurred in 2003, when the Federal Energy Regulatory Commission (FERC) published online the entire body of 1.6 million e-mails sent and received by 176 Enron employees between 2000 and 2002. Following petitioning by the company and its employees, 8 percent of those e-mails were removed from public display—notably messages containing all of the employees' social security numbers—but indications were that only one-third of the requested deletions would be made permanent. The regulations facilitating this publication of e-mails concern "business records," an unprotected category of communications including e-mails that have been read and e-mails that have been opened for more than 180 days, which are available to law enforcement agencies, lawyers, and regulators [55].

Employees can bring a case against employers based on two causes of action under common law: "the privacy tort of intrusion upon seclusion and intentional infliction of emotional distress" [50, p. 28]. Although the tort of intrusion upon seclusion is the claim more likely to be utilized, in practice it has not

usually proved successful [23]. "To apply the tort of inclusion upon seclusion to email privacy, an employee whose email is covertly monitored must demonstrate three things: 1) an intrusion, 2) an intrusion into a private affair or concern, and 3) that the intrusion would be highly offensive to a reasonable person" [56, p. 52].

It can be seen that over the past decade much thought has been given to the use and abuse of e-mail and the rights of employees to privacy in various countries, but that ample opportunity remains to consider it further and to incorporate it into national legal frameworks. It is outside the scope of this article to discuss the problems associated with the different jurisdictions under which the actions may fall when the e-mail and employment is international in nature, as frequently occurs in this increasingly internationalized and mobile world.

CONCLUSION

Privacy issues concerning the problems of monitoring and surveillance of employee e-mail still remain controversial and require more examination. On the one hand, it is argued that employers have the right to monitor their employees' activities at work to prevent misuse of business systems for personal purposes, to preserve their business security and integrity, and to maintain an efficient and competent workforce. On the other hand, the personal privacy of an employee is often considered a moral right regardless of the situation or circumstances, and as such there is a presumption against its infringement.

Conflicts between the interest of the employer's security and the employees' right to privacy can be resolved by adopting an Internet and e-mail policy and making sure that employees understand and agree with it. Both employer and employee will benefit from a clearly stated e-mail and Internet-use policy. Personal use of the Internet in the workplace may ultimately decrease; according to Eric Greenberg of the American Management Association, "as people get used to having this tantalizing equipment and access on their desks, their yen to test parameters will abate" [7, p. 33].

A number of issues remain to be researched further at the intersection of employee and employer rights. One of these issues regards the trust relationship between the employer and employees in the workplace. Employees may think their employers distrust them if they are being monitored; this may lead to loss of confidence in their work performance or potentially even induce them to become less trustworthy, in which case they will require more monitoring. In the long run, it would appear that workplace surveillance and monitoring could result in a breakdown in trust, and consequently loss of business productivity and efficiency. This potential consequence needs to be balanced against the common recommendation that employers warn employees that all communication on company equipment and time are being recorded and may be monitored or examined (whether or not such recording and monitoring actually occurs, such a policy is held to discourage personal use).

Another critical issue is the lack of relevant legislation that deals directly with the privacy issues in workplace surveillance. Although legislation can protect personal privacy, no single piece of legislation is particularly focused on the workplace implications of computer technology as discussed here. It is becoming increasingly evident that laws require modification to include the contemporary ethical implications of privacy and computer technology. It remains to be seen whether sluggish legal and judicial systems can keep up (or catch up) with the rapid evolution of information and communication technology.

A complicating factor is the increasing prevalence of satellite, communal facility, and work-at-home arrangements. Each features unique circumstances that compromise the employer's potential right to monitor, while simultaneously presenting employees with increased opportunities to use employer facilities (including Internet access) for personal ends. For example, what rights does an employer have to monitor an employee sent on assignment as a consultant working in the offices of a client in another state, who uses e-mail as the primary means of keeping in touch with family and friends as well as colleagues? Where employment contracts are based on accomplished work (piece rate or project completion), there are fewer questions about application of time and resources than there would be in straight hourly pay situations.

The constantly diversifying and extending capacities of the Internet for communication will further complicate and provide new opportunities for research in this area. Instant messaging is supplementing, and in some cases replacing, e-mail as a means of staying in touch, both from work and at home. Cell phones and handheld personal digital assistants that merge the capabilities of telephones, Internet terminals, calendars, calculators, translators, and cameras bring with them a host of new questions about privacy and which devices should be permitted under which circumstances (e.g., camera phones are not permitted at many swimming pools, yet they may also be capable of e-mailing, so such prohibitions remove e-mailing capabilities as well as photography). The potential for the most integrated devices to be banned in widely varying situations could militate for greater liberty in use of the entire range of tools, especially given the increasing difficulty in distinguishing which features are present in which physical units. Should an employer ban all small electronic devices if there is the possibility that a cell phone with camera could be used to e-mail corporate secrets (intellectual property) to an external recipient?

A fifth major area where further research is warranted is in extending the international comparison and examining the increasing role of international standards and harmonization agreements, including policies developed by the European Union and the United Nations, as well as standards promulgated by the International Organization for Standardization (ISO), and the role of national defense agencies (e.g., Department of Homeland Security in the U.S.) and criminal investigation branches of governments. The degree of interagency, international, and intersectoral cooperation in deciding which e-mails are personal and

which are business, whether illegal or immoral activities are being conducted through e-mails, and who has the authority to gather, store, and analyze such messages will occupy privacy advocates and government officials throughout the foreseeable future. Increasing governmental efforts to defeat terrorism, control nuclear weapons knowledge dissemination, inhibit currency laundering, and limit drug trading (both illegal and pharmaceutical) imply that enhanced monitoring of electronic communications of all forms is likely, potentially leading to greater employer use of the perception that such surveillance is inevitable as a justification for monitoring employee e-mails.

Everyone needs to be aware of how much privacy is leaking out through the use of the Internet and e-mail, a powerful communication tool that hundreds of millions of people use every day. The consequence of personal privacy being invaded should not be overlooked, since any electronic mail messages might one day be disclosed for publication, ridicule, or criticism. Employers are generally safe if they get the applicant's written consent to the monitoring of e-mail and investigate only information relevant to the job. Employees should have certain rights to privacy even at the workplace, but they do not have the right to misuse any of the business facilities and premises for unauthorized personal use. It is our hope that the insights provided here will deepen understanding of the key issues at the intersection of personal privacy, employer rights, and advancing electronic communications technology, leading to a clearer mutual appreciation (by both employees and employers) of their legal rights and obligations regarding personal e-mail privacy in the workplace.

ENDNOTES

1. Getting Tougher on Work Emails, *Security*, *37*(9), p. 116, 2000.
2. D. Banisar, *Privacy and Human Rights 2000: An International Survey of Privacy Laws and Development*, Privacy International, 2000. Available online at: http://www.privacyinternational.org/survey/phr2000/overview.html.
3. E. J. Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, *New York University Law Review*, *39*, pp. 962-1007, 1964.
4. P. Kovatch, Privacy Rights in the Workplace: Constitutional and Statutory Consideration, *Journal of Individual Employment Rights*, *9*(1), pp. 3-12, 2000.
5. *The Australian Privacy Charter,* The Australian Privacy Charter Group, Law School, University of New South Wales, Sydney, Australia, 1994. Available online at: http://privacy.org.au/apcc/Charter.html..
6. A. F. Westin, *Privacy and Freedom*, Atheneum, New York, 1967.
7. J. Greco, Privacy: Whose Right Is It Anyhow? *The Journal of Business Strategy*, *22*(1), pp. 32-35, 2001.
8. A. Dunn, Think of Your Soul As a Market Niche, *The New York Times*, 11 September 1996. Available online at: http://www.nytimes.com/library/cyber/surf/0911surf.html.
9. M. Pastore, Internet, E-Mail Taking Over Office Communication, *ClickZ Stats*, 7 August 2000. Available online at: http://www.clickz.com/stats/markets/professional/article.php/431931.

10. The Digital Future Report: Surveying the Digital Future—Year Four: Ten Years, Ten Trends, USC Annenberg School Center for the Digital Future, September 2004.
11. S. Gaudin, Market Opens as Nearly Half of Workers Without E-mail, *ClickZ Stats*, 14 November 2003. Available online at: http://www.clickz.com/stats/markets/professional/article.php/3099441.
12. R. Mark, Office Limits on Net Aren't Productive, *ClickZ Stats*, 6 February 2003. Available online at: http://www.clickz.com/stats/markets/professional/article.php/1580521.
13. J. H. Shannon and D. A. Rosenthal, Electronic Mail and Privacy: Can the Conflicts be Resolved? *Business Forum*, *18*(1-2), pp. 31-34, 1993.
14. J. Magney, Computing and Ethics: Control and Surveillance Versus Cooperation and Empowerment in the Workplace, in J. M. Kizza, ed., *Social and Ethical Effects of the Computer Revolution* (pp. 200-209), North Carolina: McFarland, Jefferson, 1996.
15. T. A. Shumaker, An Employee Privacy Policy Fairly Applied Can Prevent Privacy Litigation, *The National Public Accountant*, *47*(2), pp. 32-34, 2002.
16. D. Beckman and D. Hirsch, Security or Snooping? Monitoring Staff E-mail is Easy Now, But Privacy May Suffer, *ABA Journal*, *87*, pp. 72-73, April 2001.
17. S. Warren and L. Brandeis, The Right to Privacy, *Harvard Law Review, 4,* p. 193, 1890.
18. F. C. Morris Jr., The Electronic Platform: Email and Other Privacy Issues in the Workplace, *Computer and Internet Lawyer*, *20*(8), pp. 1-9, August, 2003.
19. M. Toten, Minding Your Own Business, *Australian CPA*, *70*(5), p. 48, 2000.
20. J. Waltemath, Policing Cyberspace, *Advisor Today*, *96*(11), p. 114, 2001.
21. S. Miller and J. Weckert, Privacy, the Workplace and the Internet, *Journal of Business Ethics*, *28*(3), pp. 255-265, 2000.
22. J. King and S. Ulfelder, On the Spot, *Computerworld*, *35*(6), pp. 42-43, 5 February 2001.
23. J. C. Sipior and B. T. Ward, The Ethical and Legal Quandary of Email Privacy, *Communications of the ACM*, *38*(12), pp. 48-54, 1995.
24. The UCLA Internet Report: Surveying the Digital Future—Year Three, UCLA Center for Communication Policy, January 2003.
25. S. P. Weisband and B. A. Reinig, Managing User Perceptions of Email Privacy, *Communications of the ACM*, *38*(12), pp. 40-47, 1995.
26. Major Cause of Spam: Your Employees, Research Report, Jupiter Media, Darien, Connecticut, 30 May 2002.
27. T. Phillips, Should Personal Emails Be Banned? *Director* (London), *56*(2), p. 44, 2002.
28. CCH Incorporated, Cyberspace and the Workplace: CCH Offers Tips for Creating Effective E-mail, Internet Use Policies, Riverwoods, Illinois: CCH Incorporated, 7 June 2001. Available online at: http://www.cch.com/press/news/2001/20010607h.asp
29. J. Thaddeus, Reading Employees Their E-mail Rights, *Computerworld*, *35*(3), p. 66, 15 January 2001.
30. S. J. Milberg, H. J. Smith, and S. J. Burke, Information Privacy: Corporate Management and National Regulation, *Organization Science*, *11*(1), pp. 35-57, 2000.
31. Privacy Act 1988, Act No. 119 of 1988 as Amended, Office of Legislative Drafting, Attorney-General's Department, Canberra, Australia, compilation prepared 27 April 2004 incorporating amendments up to Act No. 49 of 2004.

32. 2004 Review of the Private Sector Provisions of the Privacy Act, Office of the Federal Privacy Commissioner, Government of Australia, 20 August 2004.
33. C. Louw, Email Surveillance Under Scrutiny, *Australian CPA*, *74*(6), pp. 46-47, July 2004.
34. Protecting Your Privacy on the Internet: Canada's New Privacy Law, Office of the Privacy Commissioner of Canada, 2004. Available online at: http://www.privcom.gc.ca/fs-fi/02_05_d_13_e.asp
35. Privacy Info Canada Web Site by Professor Michael Geist of the University of Ottawa, Faculty of Law, http://www.privacyinfo.ca/, 15 October 2004.
36. D. J. Corry and K. E. Nutz, Employee E-mail and Internet Use: Canadian Legal Issues, *Journal of Labor Research*, *24*(2), pp. 233-256, 2003.
37. 15th Statistical Survey Report on the Internet Development in China, China Internet Network Information Center, Beijing, January 2005.
38. R. Greenspan, China Pulls Ahead of Japan, *ClickZ Stats*, 22 April 2002c. Available online at: http://www.clickz.com/stats/sectors/geographics/article.php/5911_1013841.
39. Population Explosion!, *ClickZ Stats*, 8 February 2005. Available online at: http://www.clickz.com/stats/sectors/geographics/article.php/151151.
40. J. Aujezdský, Skutečně muže zaměstnavatel číst vaši poštu?, *Lupa*, 15 January 2004. Available online at: http://www.lupa.cz/clanek.php3?show=3179.
41. Europa, European Union Online Knowledge Base, www.europa.eu.int/, 15 October 2004.
42. Proposal for a Decision of the European Parliament and of the Council on Establishing a Multiannual Community Programme on Promoting Safer Use of the Internet and New Online Technologies, Commission of the European Communities Document COM(2004) 91 final, 12 March 2004.
43. Bill of Rights Act 1990, Ministry of Justice, Government of New Zealand, 1990.
44. Human Rights Act 1993, Government of New Zealand, 1993.
45. Privacy Act 1993, Government of New Zealand, 1993.
46. Employment Contracts Act 1991, Government of New Zealand, 1991.
47. Employment Relations Act 2000, Government of New Zealand, 2000.
48. G. Tyler, Email Privacy—RIP, *Management Services*, *44*(10), pp. 18-20, 2000.
49. Defamation Act 1996. Her Majesty's Stationery Office, Government of the United Kingdom, 1996.
50. B. L. Scott, Employee E-mail: A Protected Right to Privacy? *Journal of Individual Employment Rights*, *9*(1), pp. 27-37, 2000-2001.
51. M. J. Camardella, Electronic Monitoring in the Workplace, *Employment Relations Today*, *30*(3), pp. 91-100, 2003.
52. D. R. Nolan, Privacy and Profitability in the Technological Workplace, *Journal of Labor Research 24*(2), pp. 207-232, 2003.
53. A. Yegyazarian, Is Your Personal E-Mail Really Private? *PC World*, 4 August 2004. Available online at: http://www.pcworld.com/news/article/0,aid,117159,00.asp.
54. *Tech Law Journal Daily E-Mail Alert*, *950*, 2 August 2004.
55. N. Swartz, The Electronic Records Conundrum, *Information Management Journal*, *38*(1), pp. 20-24, 2004.

56. Restatement (Second) of Torts 652B, 1977, cited in J. C. Sipior and B. T. Ward (eds.), The Ethical and Legal Quandary of Email Privacy, *Communications of the ACM*, *38*(12), pp. 48-54, 1995.

Direct reprint requests to:

André M. Everett
Department of Management
University of Otago
Box 56
Dunedin 9001
New Zealand
e-mail: aeverett@business.otago.ac.nz