Chapter 9
Monitoring Employee's E-mail: An E-privacy Concern

Yimeei Guo and Ying Luo

Abstract Monitoring employees is a standard practice in many workplaces, although the reasons for monitoring can vary greatly. While there is no doubt that employee monitoring is becoming a standard practice, companies need to ensure that it complies with legal requirements and does not unduly affect the employment relationship. Viewing from the protection of e-privacy in the workplace, this article discusses the notion of privacy and e-privacy at first, then examines law governing employee monitoring in various jurisdictions mainly in Germany, USA, and China as well. Finally, this article provides corporate operators some practical guidance on achieving compliance.

Keywords Employee monitoring · E-privacy · Practical guidance

9.1 Introduction

Monitoring employees is a standard practice in many workplaces, although the reasons for monitoring can vary greatly. Some company monitors to protect employees, for example, where they work in hazardous environments, and it is essential to ensure that safe working practices are being followed. Others may be under legal or regulatory obligations to monitor, for example, in the financial services sector. Most companies, however, primarily monitor to check their employees' performance. Monitoring may also be specifically targeted, for example, to detect misconduct or to ensure compliance with certain company policies and procedures.

(Published by "Proceedings of the 3rd international conference on innovation & management", Vol. II, 2006.12.1-3, pp.1011–1098**,** <ISSHP indexed>).

Y. Guo (✉) · Y. Luo
Management Science Department, Xiamen University, Xiamen 361005,
People's Republic of China

Y. Guo (ed.), *Research on Selected China's Legal Issues of E-Business*,
DOI 10.1007/978-3-662-44542-6_9

According to a most recent investigation involving 406 US and British companies which have more than 1,000 employees (*Proofpoint, 2006*), over 1/3 of such companies appointed personnel to monitor their employees' e-mail. Although the advantages to the company may be obvious, the adverse impact of monitoring employees is perhaps less apparent. A company may view employee monitoring as essential to the effective and efficient running of its business. However, if employees are permitted to use telephones, e-mail and Internet for personal use, it may be difficult for companies to draw a distinction between work and private information and activity, and limit monitoring to the former. On the contrary, even though employees may expect and accept the monitoring of their work, monitoring of their private information and activity is likely to be much less welcome.

A company's failure to consider the adverse impact of monitoring on employees can interfere with, or ultimately destroy, working relationships; it can also amount to a criminal offense. For instance, in May 2005, the former CEO and five other executives of Sonera, the Finnish telecom company, now TeliaSonera, were given fines or between 6 and 10 month suspended sentences by a Finnish court for illegally keeping logs on e-mails and telephone numbers dialed by employees, in an effort to identify who had leaked information about management disputes to mass media (Wugmeister et al. 2005).

Viewing from the protection of e-privacy in the workplace, this article discusses the notion of privacy and e-privacy at first, then examines law governing employee monitoring in various jurisdictions mainly in German, USA, and China as well. Finally, this article provides corporate operators some practical guidance on achieving compliance.

9.2 What Is Privacy/E-privacy?

The notion of privacy was first postulated in a Harvard Law Review article (Warren and Brandeis 1890), which described privacy as "the right to be let alone" when they were offended by press coverage of their families, and by "recent inventions and business methods." It took almost 20 years before the American courts issued judgments which adopted that principle.

Later on in another article (Prosser 1960), four different types of invasions of privacy were pointed out, including:

- appropriating an individual's name or likeness for commercial benefit;
- unreasonable intrusion or interference with an individual's interest in solitude or seclusion;
- publicly disclosing private facts; and
- publicly placing an individual in a false light.

From an information technology (IT) perspective, a much better definition of privacy has been that of Alan Westin, where he described privacy as: "The claim of individuals, groups, or institutions to determine for themselves when, how, and to

what extent information about them is communicated to others." This definition embodies the concept of *"fair information practices"* which forms the basis for many of the regulatory and voluntary data protection schemes.

In short, "privacy" is not just a matter of what is kept secret. In the context of e-commerce/e-business and e-government, the right to privacy, i.e., e-privacy is really *"the right to control the use of personal information"* that is disclosed to others.

9.3 E-mail Monitoring Regulations in Various Jurisdictions

9.3.1 Germany

In Europe, the general right to privacy is derived from the European Convention on Human Rights, which governs Council of Europe member states, and the Data Protection Directive (*95/46/EC*), applying to EU member states. There are differences, however, in the way that EU member states such as France, Germany, Sweden, and the UK have implemented the provisions of the Directive. To save the length, this paper chooses Germany as an example.

The monitoring of employees' Internet use is governed by employment law, collective agreements, data protection legislation, constitutional and human rights law, and telecommunications law. The result is complex, and whether the Internet use can be monitored depends on a number of individual circumstances.

As the constitutional and human rights law overlays all other regulation, the general view is that blanket monitoring infringes an employee's rights and, because they cannot be waived, collective or individual agreements to monitor Internet use are unlikely to be valid.

The Telecommunications Act 2004 (*the Act*) specifically provides for the privacy of electronic communications. It is largely thought that, by expressly or impliedly permitting private use of the Internet by employees, a company becomes a provider of telecommunications services to them. The privacy right under *the Act* can be waived, within the limits of constitutional boundaries, but a company that has tolerated private Internet use at work without an express written policy may find itself in a difficult position, because it would already be bound by *the Act*, and a change of policy might be met with resistance from the workforce or the works council.

Where a company has expressly forbidden private use of the Internet at work, data protection law, employment law, and the constitutional principles combine to form a set of complicated rules. In essence, where there is no express Internet monitoring agreement, individually with the employee or collectively with the works council, monitoring is only allowed to the extent that it is based on a concrete suspicion against an individual employee for breaching the Internet policy, or it is necessary to assess the employee's performance due to the nature of his job. Any monitoring must be kept to the necessary minimum and must be announced in advance. If a works council exists, it must expressly consent to each individual monitoring measure.

Because of the limited rights of companies to monitor, express agreements with employees or works councils are advisable. However, there is a risk that agreements will be void on the basis that they were obtained under duress, especially if they are wide-ranging and presented as a condition of employment. An express detailed agreement with the works council on a policy for the use of technology and its enforcement is usually the best way forward.

9.3.2 US

US law generally allows monitoring of employees provided they have no reasonable expectation of privacy. As a result, if companies have given employees clear notice that they will monitor public areas and technology resources, employees generally will have no reasonable expectation of privacy and a company can monitor.

Under federal law, corporate monitoring of e-mails is governed primarily by the Electronic Communications Privacy Act of 1986 (*18 USC §§ 2510 et seq.*) (*ECPA*). What a company can monitor turns on whether the employees' messages are intercepted during transmission or are retrieved from storage on the company's server.

Interceptions of online communications (that is, monitoring messages as they are transmitted) are subject to the most stringent restrictions of *ECPA* and are permitted only in limited circumstances. For employers' purposes, the exceptions most likely to apply are as follows:

- Prior consent is given by at least one party to the communication.
- Interception is necessary to provide the service or to protect the rights or property of the service provider.

Employee communications stored on a company's server can be read by it regardless of whether either of the above exceptions applies. The company is therefore relatively free to monitor stored e-mails as long as the expectation of privacy has been removed (*Fraser v Nationwide Mutual Insurance Company, 352 f.3d 107 <3rd Cir 2003>*).

Similarly, if a company provides, in its technology use policy, that it reserves the right to, and will in fact, monitor employees' Internet use, there are few legal impediments to that monitoring.

9.3.3 China

The law on employee monitoring varies significantly between different Asia-Pacific jurisdictions. Several have adopted a model similar to the USA, where giving notice to the employee is a necessary and sufficient requirement for the company to monitor. Others, such as Hong Kong and Japan, have adopted

far-reaching guidelines supplementing the legislative framework and imposing strict requirements on data collected from employees. South Korea's approach is more similar to that taken in Europe. Here, this article takes China including Hong Kong, Mainland China, and Taiwan as a sample for discussion.

According to a Web@Work survey (*Websense, 2005*), across eight regions of the world, 83 % of respondents said they surfed non-work-related Web sites during office hours. Chinese office workers are the worst, concludes the survey, because they spend more than 1 h a day on personal usage. Specifically, Chinese employees spend 5.6 h per week on personal Internet usage in the workplace, 1.4 h more than the average of 4.2 h for companies in the Asia-Pacific region.

But employers in China are taking notice. For instance, Ruideng Communications, a Sichuan company, recently installed eight micro-cameras in the ceiling, overlooking all the office's computers. Productivity has shot up, but some employees feel uneasy about the surveillance and have complained about a "loss of privacy." TCL, the world's largest TV maker, has a strict policy on Web access. Its IT department uses specially designed software to track and record all online activities of all employees. TCL R&D staffs are not allowed to use third-party instant messenger (IM) platforms such as MSN.

As pointed out by one legal expert (Zhao 2003), whether or not business security or employee's privacy is indeed more important is not clearly provided by law in Mainland China. By referring to foreign legislative examples, it is the basic solution to solve such problem to award a right for business to monitoring its employee's e-mail under certain conditions and make a clear cut between infringing citizens privacy right and maintaining business' sound interest.

In Hong Kong, the Personal Data (Privacy) Ordinance 1997 (*the Ordinance*) applies to employee monitoring and allows the Privacy Commission for Personal Data to adopt guidelines. In December 2004, the Privacy Commissioner adopted guidelines on employee monitoring of e-mail, Internet, and telephone use and CCTV monitoring.

There are potentially serious consequences if *the Ordinance* requirements are not met. A company may be exposed to:

- Civil compensation to individuals who suffer damage.

Enforcement notices served by the Privacy Commissioner (for example, when an aggrieved party complains). Non-compliance with an enforcement notice carries a penalty of between HK$25,001 (about US$3,200) and HK$50,000 (about US$6,400) and 2 years' imprisonment.

As to Taiwan, although there is a constitutional right to privacy (*Article 12, Constitution 1946*) and detailed data privacy legislation has been in place since 1995, the clearest statement of employee privacy law is found in Taipei district court case law in 2003 adopting the reasonable expectation test.

Under this test, one company can only monitor employees' e-mails if they do not have a reasonable expectation of the privacy of their work e-mails (for example, where employees have been provided with a clear e-mail monitoring policy).

9.4 Conclusion and Suggestion

Even where companies can justify monitoring employees' activities, it may still be advisable for them to strike a balance between the legitimate need to run their businesses in the best way they see fit and respect for their employees' private information and activities. While there is no doubt that employee monitoring is becoming a standard practice, companies need to ensure that it complies with legal requirements and does not unduly affect the employment relationship. Here, this article tries to put down some tips for companies' compliance as follows:

9.4.1 Providing Notice by Implementing and Disseminating a Technology Use Policy

Notify employees of any anticipated intention to monitor. This overcomes any employee expectation of privacy in using the company's e-mail or accessing the Internet while at work. If a halfway approach is taken (for example, by allowing employees limited personal use of IT equipment), a company policy should be clearly set out.

9.4.2 Stating the Reasons for the Monitoring

Include in any e-mail or Internet use policy a statement of the reasons for monitoring (for example, to ensure compliance with company policies or the proper functioning of the computer systems, or to monitor an employee's performance).

9.4.3 Proportionality of the Monitoring

Be clear about the reasons for monitoring. In principle, monitoring should be limited to the extent necessary to achieve a certain legitimate aim. If it can be carried out on a less intrusive basis (for example, monitoring only the number of e-mails sent or amount of time spent on the Internet), then this should be used. Ensure that local laws can be complied with once the personal data has been collected (see below).

9.4.4 Complying with Local Laws

Provisions vary dramatically between jurisdictions. Do not ignore local laws and adopt, for example, a US approach across jurisdictions. Such an approach runs a serious risk of non-compliance.

As well as complying with any notice requirements, remember that many jurisdictions require a legal basis for monitoring, such as employee consent, or conducting a balance of interest test where the company's interest in monitoring outweighs the employee's right to privacy. Verify whether there are any applicable exceptions for employee monitoring.

9.4.5 Conduct Training

Once a policy is implemented, conduct training sessions to raise employees' awareness of monitoring and its purposes.

9.4.6 Audits

Conduct regular audits at least annually to ensure that policies are current, applicable, and being followed (Wugmeister et al. 2005).

References

1/3 of US and British companies stole a Glance at their employees' E-mail, Beijing Youth Times, http://www.ynet.com/view.jsp?oid=9647857, 6 June 2006.

Boufford, John G. 1998. Privacy on the information highway. *University of New Brunswick Law Journal* 47: 219.

Prosser, William. 1960. Privacy. *California Law Review* 48: 383.

Wugmeister, Miriam, Ann, Bevitt, Peter J. Edlind, and Ritter, C. 2005. *Employee monitoring: Highlighting the issue*, http://www.mofo.com/news/updates/files/update02051.html, Aug 2005.

Warren, S., and Brandies, L. 1890. *Privacy, Harvard law review*. pp. 207–208.

Westin A.F. 1967. *Privacy and freedom*. New York: Atheneum, at 7.

Zhou, Raymond, and Zhuoqiong, Wang. 2005. Chinese office workers world's worst in cyber slacking, China Daily page 1. http://www.chinadaily.com.cn/ english/doc/2005-08/18/ content_469947.htm. 18 Aug 2005.

Zhao Limei. 2003. *Analysis and research on legal problems about E-mail (in Chinese)*. http://tech.sina.com.cn/news/review1/2000-04-21/23363.shtml, 13 May 2003.