

Company Employee Privacy Strategy

Yu Zhang

Department of Computer Science

Telecommunications software and multimedia laboratory

Helsinki University of Technology

Yuzhang@cc.hut.fi

Abstract

With the development of human right, employee privacy is an evolving issue, which face nowadays employers and employees. There are always conflicts between employers and employees on how employee privacy is. Employers want to measure employees' performance and monitor suspicious or illegal activity that could cause direct business loss. Employees want their interests and privacy to be taken into account and respected. In this study, we try to find how to implement employees' privacy to ensure the employee moral, and at the same time ensure the effective business management.

1. Introduction

What is privacy? The privacy law in U.S.A give such definition: "*Privacy* is the expectation that confidential personal information disclosed in a private place will not be disclosed to third parties, when that disclosure would cause either embarrassment or emotional distress to a person of reasonable sensitivities. *Information* is interpreted broadly to include facts, images (e.g., photographs, videotapes), and disparaging opinions." [1]

For employees, privacy means more things than the previous definition, including private information and data, private use of Internet and private email, phone calls, private files stored in the company-provided computers, etc. The increasing problems or claims about employee's privacy mostly are that employers have not respected their employees' strong desire for privacy, or they have not taken the necessary steps and policy to protect that privacy. There are many real cases about the conflict of employees' privacy between employers and their employees.

Through the studying, we find that the two basic problems are: *There is no definition about what employee privacy is.* Employers and employees may have different views on how much personnel privacy employees should have, what personnel information and data employers should gather and protect. Second, *there is no standard policy to define how to implement employee's privacy and no standard privacy policy available to fit all possible cases that may arise.* All these problems and unclear things cause the claims and conflict occur.

Our research is aimed at solving these two problems through analyzing the different views and handling ways in different places.

The study concentrates on the situations in the USA, Europe Union (EU) and Finland. Asia and Africa are not in the consideration because of the different culture. Meanwhile, the study focuses on the employees who work in private companies. The employees in government departments are not in the consideration. The information

provided in this article is not intended to be legal advice and should not be relied upon as such.

The rest of the paper is organized as follows. In section 2 we present the different views on employees' privacy; the different views contain employer's view, employees' view, and government's view. We make our definition of employees' privacy according to these different views. In section 3 we discuss how employer handle employees's privacy in correct way. First we divide employee privacy into different categories, then give the solution for each category. In section 4 we draw our conclusion.

2. Different view on employee's privacy

Employee privacy involves serveral different views, government, law, employers and employees. Each has its own opinions on employee's privacy. In the following chapter, we see the different views.

2.1 Employer's view on employee's privacy

First we look at employers' view on employee privacy.

Most employers think that the employees should not have too much privacy, especially for enterprises facing an economic slowdown. They have reasons for their issue: First, employers have strong interest in ensuring that their employees are productive, loyal, law abiding and capable. Second, employers want to cut costs, increase productivity, prevent workers from doing anything illegal or immoral and prevent abuse of the company-provided systems and (e.g., sending harassing e-mail, trade secrets or copyrighted material).

So, most employers do not respect their employee's privacy too much. All what employer did can be divided into three types.

First, employers try to gather and access personal and sensitive information of their employees. When they hire an employee, they want applicants to answer questions, such as education background, work record, criminal, credit, health, marriage, family background, etc. And in many big companies, the applicants must take psychological tests before they getting job. Sometimes employers even want to hire private investigators to observe their employees or search their property. This results in that the conflict between employers' interest in obtaining information about employees and employees' interest in privacy is being resolved in the courts with greater frequency.

Second, employers disclose employees' private information on purpose or by accident. Publication or disclosure of private facts about an employee to others within the company may be sufficient to state a claim, especially if the disclosure is made to individuals who do not have a legitimate need for the information. The disclosure to others outside the company is more serious.

Third, employers monitor employees' activities at workplace. More and more employers measure employees' performance and monitor suspicious or illegal activity that could cause direct business loss. They try to ensure that all activities done in the company are for business purpose. Actually, the balance between employees' rights and business interests is weighted heavily in favour of the enterprise mostly. There are different kinds of monitoring, for instance, listening to employees' telephone calls, watching them over video cameras, supervising their internet usage and network activities, checking data stored on the computers, or reading their e-mail. The development of new IT technologies allows employers to monitor many aspects of their employees' activities on employer-provided computer systems. According to the survey from the American Management Association(AMA), there are nearly 78 percent major U.S.companies record and review some sort of employee communications and activities on the job. And the workplace monitoring continues to rise.

All employers try to ensure his interest. However, most of them are not very clear what extent they can do, when they gather employees' information and monitor employees' activities. Moreover they do not know what they should do to protect employee's private information after they get them. Generally, employers should ensure that they are in compliance with all relevant laws governing privacy and responsibility in all the nations where they do business. Meanwhile, they should not affect their staff moral and motivation to work. It's a delicate balance, but it is hard to do. "When you are hiring new employees, monitoring employee performance, and investigating suspected employee misconduct, you may wonder exactly how far the law allows you to go with your inquiries." [2]

2.2 Employee's point of view on employer's privacy

We see how employees' view their privacy in this chapter.

Generally speaking, employees hope employers can respect their privacy. About the personal data and information, employees are greatly concerned about the leakage of their sensitive and non-public personal information by their employers. However, employees always suspect and trust that employer will protect and not misuse their privacy. Basically, most employees answer all the questions asked by employers and provide all the information and certificates employers require when they apply for a new job. They think their employers will treat their private information correctly. "People act as if they have privacy protection. They don't stop to think they are under scrutiny," said Stewart Baker, head of the technology law practice at Washington, D.C.-firm Steptoe & Johnson" [3].

About the workplace monitoring, no employee likes that his/her activities in the company are monitored, his/her data stored in the computer is checked and his/her Internet access is recorded. Basically, employees expect that their privacy interest be protected by employers. Most employees accept that their employers have right to monitor their activities on company-provided equipment and systems. However, they hope all the monitor is for solid reason and is limited accordingly. Moreover, employees expect that they should be specifically and properly advised in writing

through an employment contract, manual or other adequate means of written notification. In addition, private communications should not be recorded.

2.3 Government and law

In this chapter we see the governments' view on employee privacy.

More and more countries recognize that employee privacy right is an important issue. But different countries deal with this issue standing on different grounds. There is a trend toward increase privacy legislation worldwide, led by some European associations. But there are others advocating for the protection of employers' benefit in USA.

First we see the current situation in USA. From the studying, we find that the USA government pays much concern on this issue. There are very complete Federal, state and local law that specify the details related to the different employee privacy. For example, about the personal data, "The Americans Disabilities Act (ADA) has caused employers to make major revisions in their hiring process to avoid unlawful inquiries about applicants' medical conditions. Under the ADA, you may not ask applicants whether they have a disability or about the nature and severity of any disabilities. [4] "Federal and state laws limit employers' ability to obtain and use medical information about their employees and applicants for employment." [5]

About the activity privacy at workplace, the main trend in USA is that employers can monitor employees' performance at workplace. "The Electronic Communications Privacy Act (ECPA) permits employers to monitor and intercept an employee's cellular, wire or electronic communications on employer-provided systems when such monitoring is necessary for the protection of the rights or property of the employer." [6] "In an unpublished California case, the court concluded that an employer did not violate employees' right to privacy by intercepting employees' personal e-mail messages, where the employer had a written policy, signed by the employees, stating that computer equipment was to be used for business purposes only and where the employees were aware that others had access to their e-mail messages." [7] "The Fourth U.S. Circuit Court of Appeals (which governs the state of Virginia) recently addressed this issue, and the answers are good for you. Employees don't have privacy right on workplace computer" [5]

Second, we see the situation in EU countries. In EU, there is data privacy law and enterprises must ensure that personal information is properly protected (At the same time, each member of EU has its own data protection law.). Meanwhile, there is law about how to deal with monitoring at workplace. "The Privacy laws in many European countries now require that before a worker can be monitored, the requesting manager or police agency must document what information is to be collected, what they are looking for and how long the surveillance is to go on. If the request is approved, the human resources department must monitor to make sure the surveillance is not misused. Logs collected can be shown only to the people with a specific need to know and must be shown to the employee in question on request. " [8]

In addition, many developed nations enacted data protection laws that control how personal information can be used in the private sector. The EU has passed comprehensive privacy rules that can restrict the transfer of personal data to countries without equivalent levels of regulatory protection.

Moreover there are some human rights groups in the world, for instance Privacy International (in UK) to act as a watchdog on surveillance by governments and corporations for information.

2.4 Situation in Finland

In Finland, there are strong privacy regulations. For instance, there is Personal Data Act (523/1999) that aims at implementing the protection of private life and the other basic rights that safeguard the right to privacy. However, we do not find regulation about monitoring employees at workplace.

In practice, Employees' privacy gets enough respect and protection. First, employers do not collect and search sensitive data from the employees. Second, employers think that monitoring can have damaging effects on productivity and morale. So, they seldom use electronic monitors to monitor employee's activities at workplace.

Because it is hard to make the very clear line between work and private life, so there are many Finnish companies permitting occasional personal usage of Internet and E-mail. Especially the high-tech enterprises and those with salaried workers, for instance, in Nokia Ltd, employees are allowed to use email for personal purposes. In Nokia, employees' privacy is reasonable protected because employer treats employees as one of the most important asset of the company. They concern employees' satisfaction.

2.5 Definition of employees privacy

Combining different views on employees' privacy, we give a definition of it. "Employee privacy means the privacy right employee has when he works for an employer, which contains two parts. One is related to employee's personal data and information, another is employees' performance privacy at workplace and on company-provided equipments.

Employer can gather employees' general information (name, gender, age, ID number, nationality, education background, work record, criminal record). The private information such as age, security ID, education background, work record and so on should be treated as confidential. Employer is limited to obtain and use medical information about their employees and applicants for employment. Employer can make inquiry on this information when they need, however, the inquiry must be job related and consistent with business necessity. And the information obtained by the employer must be maintained in a separate file and treated as confidential.

Employees do not have any personal-privacy right on using company provided equipments(computer, mobile etc). All electronic communications systems and all information transmitted by, received from, or stored in these systems are the property of the company. These systems are to be used solely for job-related purposes. Employees have no personal privacy right in use of this equipment or with the transmission, receipt or storage of information in these equipments. Employer can monitor the use of company equipments at any time at its discretion. Such monitoring may include printing and reading all electronic mails, monitor Internet usage and activities, and monitor the communication calls. However, employer should not record or disclose private content if such content is not offensive or racially related.

It is advisable that that employer will put employees on notice of employer monitoring. ”

3. How employer handle employees’s privacy in correct way

3.1 Category of employee privacy information

Before finding the technical solution for employees' privacy right, first we should make clear what are privacy data and information.

Employees have both public and non-public data each including many items. The public data contains name, job title, company-ID, office phone number, fax number, company Email address, office site, etc. This information can be put in the company’s phone book. For the non-public data, includes birth, social security ID, home phone, salary, education background, work record and medical record (if company can get it), salary, job grade and so on, should be kept confidential because employees have privacy right on them.

Employees’ activities at workplace contain communication and working. Employees have no privacy rights on their private activities at workplace, on company provided computer and some other properties.

Figure 1 shows the categories of employees' personal data and employee activities at workplace.

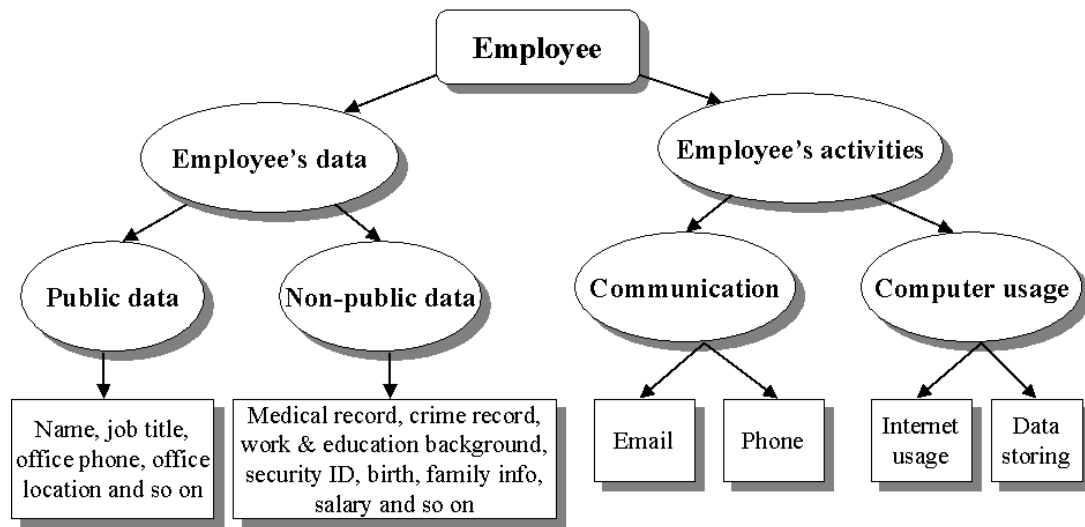


Figure 1 Category of Employee privacy

3.2 Solution

First, we present how to protect employees' personal data. It is the responsibility of employer to protect the private data of employees. There are treats for this information from both internal and external activities of the company. So, all these kind of data should be treated as confidential and kept at the special server. There should be policy and procedures to safeguard access to this personal information.

Second, we provide solution for how to prevent the misuse of Internet. There are more and more companies permitting occasional personal usage of Internet because it is hard to make a clear line between work and private life. However, the differences between personal use and unacceptable abuse must be clearly defined. In order to reduce the Internet misuse, employers can use some monitor tools to limit the web sites which employees can visit. For instance, there is such content filtering products that work by assigning categories, such as shopping, gambling, e-commerce, etc to Web sites. The manager decides which web sites to censor by simply selecting a category, and each web site assigned to that category is blocked. This filtering technology can block those inappropriate categories.

Last, building the privacy policy before monitoring. "The Company respects the individual privacy of its employees. However, an employee may not expect privacy rights to be extended to work-related conduct or the use of company-owned

equipment, supplies, systems or property." [6] However, employers should make employees privacy policy to notify employees about these practices. The first purpose of this policy is to state employer's right and intent to do randomly monitoring. The second reason is to notify employees that no reasonable expectation of privacy exists in connection with use of company's equipments, supplies, systems or property, including computer files, computer databases, telephone etc. So, whenever employees use the company's e-mail, computer or telephone systems, they are clear in mind that the company retains the right to access these systems at its own discretion to verify their proper usage. Employers can minimise their risk of legal liability through this formal written statement.

4. Conclusion

Employees have strong privacy right on their personal information, but they have little privacy on their activities at work place. Employers should establish management policies, practices that safeguard against monitoring the employee private information and activities.

Although the balance between employees' rights and business interests is weighted heavily in favour of the enterprise. However, employees' privacy protection has long-term effects on staff morale, recruitment and retention. At present, it is difficult to see how short-term gains in productivity are worth the long-term erosion of morale. So employers should respect employees' privacy, have to take the necessary steps to protect employee's privacy and avoid that monitoring become counterproductive.

However, respecting employees' privacy while monitoring abuse and enforcing policy requires a delicate balancing act. The reasonable balance point can be determined according to an enterprise's culture, regulations, technical issues, and short-term gains in productivity vs. the long-term erosion of employee morale.

Reference

[1] Privacy Law in the USA, <http://www.rbs2.com/privacy.htm> [referred 03-01-2002],

[2] Reuters, PT Employee privacy under siege, 29-05-2001, [referenced 15-10-2001], <http://news.cnet.com/news/0-1005-202-6080066.html>

[3] Hrhero.com, Employment Law Newsletters, unknown, [referenced 16-10-2001], <http://www.hrhero.com/empnl.shtml>

[4] ohn Patzakis, Esq., Employer Interests and Employee Privacy Rights in Internal Investigations Involving Computer Data, 09-04-2001, [referenced 15-10-2001], http://www.baywalk.com/legal/library/employee_privacy_rights.htm

[5] Shannon P. Garbett, Employees beware: Big Brother is watching, unknown, [referenced 20-10-2001], <http://www.hrhero.com/topics/electronic/watching.shtml>

[6] Sysco.com, unknown, [referenced 20-10-2001], http://www.sysco.com/building/building_bs_privacy2.html

[7] Jeffrey S. Portnoy, Esq. and Sarah O. Wang, Esq., Employer access Vs. Employee privacy: what information can employers obtain?, 13-10-1999, [referenced 15-10-2001], http://www.cades.com/pubs/html/emp_law4b.html

[8] Joyce Graff, Commentary: Weighing employee privacy, 10-07-2001, [referenced 22-10-2001], <http://news.cnet.com/news/0-1005-201-6538762-0.html?tag=lh>