**Data Privacy for Employees in Private Corporations**

Hema Lakshmi Prasanna Sanaka

MahendraKumar Chaudhari

Sreeja Reddy Singidi

Venkat Cholleti

Data Analytics, Webster University

CSDA 5130: Social and Ethical Issues in Analytics

Prof. Oubonvanh Douangkeomany

October 06, 2022

**Data Privacy for Employees in Private Corporations**

The development of information technology has fundamentally altered our way of life during the last 15 years (De Capitani di Vimercat et al., 2012). We may use our laptops, mobile phones, tablets, or any other device with an Internet connection to access a wide range of services and information at any time, anywhere. The advent of information technology has benefited our society, but it has also affected consumer privacy. An increasing amount of personal information is gathered, used, shared, and distributed. This includes information on demographics, health, tweets, emails, pictures, videos, and locations. There are several justifications for gathering, disclosing, and using personal data. Public, private, and governmental entities, for instance, might reveal or share their data collections for research or statistical purposes, to deliver services more effectively and efficiently, or as required by laws and regulations (De Capitani di Vimercat et al., 2012). Sharing and distributing personal data, though, could jeopardize people's right to privacy.

Information, its existence, and its usage raise a host of ethical concerns (Richard O. Mason Southern Methodist University et al., 1986) identifies these as PAPA: There are four main concerns with information: privacy (how much personal data should be shared?), accuracy (who is responsible for the authenticity, fidelity, and accuracy of information?), property (who owns information? ), and access(What kind of data may someone legally demand?) (Pelteret & Ophoff, 2016). When deciding whether to reveal personal information or maintain their privacy, people must navigate several complex issues (Pelteret & Ophoff, 2016).

Organizations cannot optimize productivity and planning without access to data about their employees. Additionally, the introduction of the GDPR law has sparked the My Data movement, which advocates for personal data that is focused on individuals (Olsen, 2020). This not only helps workers learn more about data but also gives them better access to control over that data. Positively increasing transparency and generating a good level of usability were also demonstrated by the results (Olsen, 2020).

As new technology and complicated regulations and case laws are implemented, companies worry about employee privacy. In this age of thorough background checks, rapid data transfers, and widespread social media use by employees, little advises firms on privacy, data protection, and a technologically advanced workplace. Privacy and data protection laws on a federal, state, regional, and local level must be followed by all businesses.

Internet growth threatens corporate security. Corporations are seen as non-state or mega-state entities and are attacked. They are also converging with their home state's military and industrial complexes, making the nation a target for force. Their increasing reliance on the Internet makes them vulnerable to attacks on computer networks and stored data. Physical destruction and large-scale information system crashes are common. Traditional corporate command and control structures may not be able to handle invisible or unanticipated forms of aggression. Political activists, commercial competitors, criminals, and terrorists are the new aggressors. Risk assessment and treatment must be revised. There is also a need to rethink how corporations are organized and how they handle risk. Traditional risk management is hierarchical and may not handle new threats well. If information flows poorly, a hierarchical company may be vulnerable. A networked company may be better able to withstand a crippling attack.

**Literature Review**

Information breaches both inside and outside can result in data leaks. The notion of proportionality is proposed as a basic element of an information processing regulation. A surge in insider threats has been noted, particularly in incidences of data leakage, despite the established security safeguards that organizations have put in place to safeguard their digital assets. Due to the value of information as company resources, there is an increasing need for organizations to identify, stop, and mitigate such infractions. Given the growing frequency of events and the associated costs for those affected, data leakage poses a severe threat to enterprises (Kaur et al., 2017).

Many economists are concerned about the potential for widespread exploitation of personal information by profit-driven companies when concerns about electronic information privacy first gained notice. The overall rule for handling workplace information is defined by information processing legislation, which contains the idea of proportionality as its core pillar. The effectiveness of protecting employees' personal information should be improved by considering public interest litigation as a means of improving the remedy for employee rights (Wang, 2022).

**Employee Privacy Rights**

The increasing use of technology at work has given rise to privacy issues for both firms and individuals. Businesses can dramatically save operating expenses by using email and the Internet. Both companies and employees are quite concerned about how much employers are using employee monitoring and continually expanding their capabilities. A person's right to privacy can be viewed as a right to manage who has access to them. It is a right to restrict public access to oneself, which comprises personal information that one never publishes (Moore, 2000).

Employee safety is the practice of ensuring worker safety in the workplace by establishing a safe working environment for employees. We have to ensure employee safety to enhance morale, productivity, and the business's expansion and profitability. Safety violations can have legal and financial consequences.

**Privacy Invasion**

Two revolutionary technologies—digital photography and the Internet—have grown incredibly quickly in the last ten years, transforming our culture (Shoshitaishvili et al., 2015). We now have small, integrated digital cameras with practically endless storage capacity, replacing the cumbersome film cameras of the past with limited (and difficult-to-distribute) film (Shoshitaishvili et al., 2015). People are employing these technologies to snap more and more pictures of themselves and other people using their gadgets.

**Smart Employee Monitoring**

In the past, the primary component of the modern labor scene was permanent, full-time work. People's perspectives on work have evolved as a result of remote employment like on-site work or working from home. These days, it’s not crucial for employers to show up at their jobs. "The COVID-19 pandemic has probably accelerated these changes" (Trivedi & Patel, 2021, p. 87). Employees benefit from remote employment because they can work at their own pace and save time traveling. "Employee-monitoring with the use of technology by businesses to track employees' job performance" (Trivedi & Patel, 2021, p. 87). Companies improve their productivity and make successful decisions with the help of employee monitoring. Employee monitoring tracks the live activities of employees. So, companies can see employees' performance and promote them accordingly.

Types of monitoring (Mishra & Crampton,1998):

1. Computer Monitoring: Computer software checks an employee’s efficiency to see if they are fast enough to do work successfully.

2. Video Surveillance:Companies put cameras in their companies to check the live activities of the companies like employees working or not? or who enters the companies?

3. Electronic Mail (e-mail) and Voice Mail:" E-mail provides employers with options to ask for a "Receipt Request" (Mishra & Crampton, 1998, p. 4).

4. Undercover Investigators: In some companies, managers send some "undercover investigators" to see an employee’s performance (Mishra & Clifton, 1998, p. 5). These investigators may be their coworkers or friends at other companies.

Employee monitoring has many merits and demerits.

Merits: If the manager sees the activities of the employee, then the employee does work with more focus and less time. Moreover, it helps to analyze live work activities like what types of things need to be done, employee abilities and which person can do which work. If there is a need for another person, they can hire that person. Also, if someone wants to see an employee’s information then employee monitoring notifies them about their privacy risks.

Demerits: If companies have data about employees' personal lives, like employees’ family details, then employees lose trust in companies. This also affects the employees’ work, as they may not focus more on it. When employees are under surveillance, they feel unsafe about their privacy. They have some questions in their minds, like when they are talking with the family on call, they may feel uncomfortable talking because, in their mind, they think that someone is watching or listening to them.

**Data Breaches in Private Corporations: Threats and Consequences**

"Data leakage can occur as a result of both internal and external information breaches, either intentionally (such as data theft by hackers) or unintentionally (such as employees and partners accidentally disclosing sensitive information)” (Cheng et al, 2017, p. 01). External or malignant insiders cause intentional leaks. Hacker intrusions, malware, viruses, and social engineering cause external data breaches. Third parties value private company data. They target social security numbers, contact information, birth dates, education, other personal information, financial information, health information, and other data (Cheng et al, 2017 p. 01). This information is used for tracking and blackmailing and third parties have some intention of getting money.

Data breaches have consequences for users' trust as well as companies' reputations. According to Emmanuel Elioth Lulandala, Facebook users have lost trust in Facebook. Facebook companies have a lot of information about users' personal information and activities. Moreover, "Facebook knew about the data breach since 2015 but failed to notify its users until it was whistle-blowed in 2018" (Lulandala, 2020, p. 47). Some companies wanted to get more money by sharing information, but they lost their users' trust as well as their reputation.

**Key Takeaways**

**Data Breach Reporting**

A data breach should be reported to the Information Commissioner's Office (in the UK) if it threatens people's rights and freedoms (Ashton, 2022). This should be in every country. Employees can report several types of data, such as when an unauthorized third-party accesses or modifies your personal information without your permission. The Information Commissioner's office should be notified within 72 hours of a data breach (Ashton, 2022). Also, firms must notify victims "without undue delay" if a data breach poses a high risk to their rights and freedoms (Ashton, 2022).

**Obligations of the company**

An organization should make sure that only authorized individuals have access to employee information. In many organizations, employees have to use their phones. Employees use their email accounts and other browsers' accounts on their phones or computers. So, employees should use only the company’s account or need to make a company account and they must be aware of the information that their employers collect about them. They should share only those pieces of information that are required for their companies. A company should not track personal calls, internet history, mail, and other things.

In addition to moving throughout an organization, if data is enhanced or connected to another data record, its nature also changes. One kind of data is a social security number. If the record is connected to the person's driver's license, additional information about them is known, making the record richer and more sensitive. Inform every employee on the importance of sensitive data, the necessity to secure it, and the proper way to handle data for their position. Data is no longer just information; how it is used or abused has the power to alter lives.

**Analysis**

**Employee Data Protection**

‘Three significant firms have made the initiative to develop more detailed workplace guidelines. They are Council of Europe, EU, and ILO’ (Hendrickx, 2022).

The global key principles are listed below (Hendrickx, 2022):

1. Fairness: Personal information should be handled fairly (with links to non-discrimination, transparency, and the absence of fraud).

2. Legitimacy: Also known as lawfulness, this refers to how properly or legitimately personal data is managed.

3. Purpose specification: Personal data should only be processed for clear, explicit, and legal purposes.

4. Proportionality: When processing personal data, it is important to keep in mind general proportionality rules, data reduction rules, rules for non-excessive processing, and rules for relevance to purpose.

5. Data quality: Personal information must be true, comprehensive, and current.

6. Openness and transparency: All frameworks have some level of openness or transparency. There are a variety of obligations, from broad ones like having open policies and making sure that information regarding the processing of personal data is made public to more particular ones like lists of information that must be sent directly to data subjects.

7. Security: Personal data should be protected with adequate (or sufficient) safeguards (processing).

8. Data retention: Personal information shouldn't be kept around longer than is required for processing.

9. Accountability: (a slightly less common principle, with six out of ten frameworks) ensuring that data controllers (and, where appropriate, processors) are accountable for the personal data they process.

10. Access: Data subjects have the right to access their personal information and to have it corrected, deleted, or otherwise destroyed, with (for some instruments) the additional assurance of objecting to or contesting the processing of their data.

**Practical Implications**

The organization's health is the responsibility of senior management. For the business to succeed, it must clearly define its direction. Several policies lay out the aim in detail. The policies will convey specific information to coworkers and outside parties. To internal parties, influencing and dictating their course of action is the goal of the policies. To advance the goals of the company, management thus indirectly directs employee behavior.

Through policies, management often establishes the company's vision, rules, and regulations (von Solms & von Solms, 2004). These policies should offer direction to partners and workers on how to conduct themselves in a way that complies with management's expectations.

Effective design and implementation of the policies are required to account for changing economic and technology trends. The existence of a set of corporate policies does not guarantee that everyone will abide by them. To ensure proper behavior, these principles should ideally be reflected in some aspect of the company culture. An internal set of regulations that establishes the organization's norms and expectations are company policies and procedures. They assist in letting staff members know what they are permitted and cannot accomplish along with the proper procedures. Creating common assumptions that are suitable for management and teammates is a difficult process. The management would outline their expectations of the group members in a set of policies. Particularly in terms of fundamental presumptions and ideas, these policies must be supported by the group members.

Business rules have gained popularity over the past few decades, mostly because they enable systems to be flexible and adaptable to change. But business regulations don't apply to IT or the application software it uses. Since the business is the one that establishes and owns the rules, it must also administer them. The rule’s origins are found in the field of artificial intelligence, where they have been effectively used as a knowledge representation mechanism. The expertise of a human specialist can be recorded and stored in the form of intricate networks of rules in knowledge-based systems. Declarative languages, which don't imply chronology or flow of control, are frequently used to define the rules. A lot of work has gone into developing a reliable and effective mechanism for representing business requirements in database systems since the concept of integrating business rules in database systems first surfaced.

There were also business norms in the object-oriented community. Although it appears that supporters of object-oriented techniques concur that business rules need consideration, they continue to argue about where to place them in object-oriented models.  Some people think that since objects are in charge of their data and behavior, business rules ought to be modeled as attributes of classes in object/class models. Many paradigms, including business norms, are being combined by others to attain harmony (Bajec & Krisper, 2005).

On the market, there are countless software and hardware options for monitoring a wide range of activities. Software for monitoring or surveillance is available for several thousand dollars to absolutely nothing. The majority of solutions can record keystrokes typed, website and application usage, in-depth file usage, incoming and outgoing chat, and email traffic, internet connections, windows that were used, internet packet data, screenshots of the desktop, program installations, and much more. All recorded activity can be displayed by the software in simple-to-read graphical reports. Employers can set up particular alerts to inform management when an employee takes on a certain activity or may not be hitting productivity targets. It's also crucial to remember that many employers use video and telephone monitoring in addition to computer usage tracking.

Companies may quickly and covertly establish sophisticated monitoring systems, enabling employers to keep an eye on employees without their awareness. The company can remotely install software that is invisible to computer users or can deploy hardware equipment at the firewall that will monitor all electronic transactions. In every country in the world, both big and small enterprises use employee monitoring.

**Future Research Considerations or Implications**

A company can now monitor an employee's behavior using innovative technical tools like video monitoring and GPS location. For example, like Uber company, a company can check the speed limit of an employee's car and give a notification an alert when it reaches a high speed. Also, while driving, if an employee uses a mobile phone, the company can remind them not to use a mobile phone. In the event of an employee's car accident, a company can help them by providing emergency health care or calling an ambulance.

However, when an employee is not at work, it is possible to track their activities. Therefore, there should be some limit to the use of technological tools for monitoring an employee's activities. For example, a company should use these properties for its business purposes and during working hours. Moreover, a company should notify an employee regarding their information, like how it will be used and how it will be important for business.

There are some guidelines an employee and a company need to follow. To begin with, companies should make a clear and transparent view regarding employees' privacy and the company’s policies. A company should need a leader who can communicate with employees regarding their privacy and the company's goals. For communication, companies should provide personal equipment like laptops and company browser accounts. So, employees need not use their tools. There should be some mutual agreement regarding personal data between employees and companies (Adnan, 2021, p. 50).

**Conclusion**

Various methods of employee surveillance are possible. By utilizing reputable employee monitoring software, managers and business owners may easily keep track of employee behavior. Many applications and other tools exist that allow managers to digitally monitor their staff.

In the workplace, utilizing technology to monitor employees is nothing new. Examples include workplace video cameras, GPS and telemetry devices used to track corporate vehicle position and speed events, and more. The use of screen capture, keystroke tracking, mouse click as well as motion tracking, and other advanced employee monitoring technologies enables the surveillance of employees' computer behavior.

**Brief findings or key takeaways**

Businesses should carefully examine electronic staff e-mail and Internet monitoring. To keep the organization's culture intact, sensitive problems of loyalty and trust need to be addressed. Proper planning, unambiguous policies, and thorough procedures are necessary for monitoring. Both advocates and detractors of monitoring concur that businesses should have unambiguous regulations regarding electronic surveillance and that these policies should be often and effectively communicated to employees. Additionally, they concur that staff members need official training on email and Internet policies, as well as how to use them and behave. Managers and IT departments must work together to reduce the risk associated with giving employees unrestricted access to the Internet and company email systems, given the possible liabilities firms may face because of employees misusing technology resources.

There has been a rise in interest in the tension that can arise between employees' right to privacy in the workplace and employers' desire to prevent theft of business property, the disclosure of trade secrets, and the risk of expensive litigation. As a result of the legal system's generous treatment of employer monitoring of employees' electronic communications on the job, employers typically come out on top in this trade. Employees and employers often have different perspectives on monitoring, so companies need to think about how it may affect their staff.

"Privacy is a moral right, and while surveillance can be justified, an intrusion is not" (Friedman, 2007, p. 78).

**Recommendations for a path forward**

In Micro-and Small Enterprises, cybersecurity depends heavily on the human aspect and their interaction (Remmele, 2021, p. 4). "GEIGER contains easy-to-use software for monitoring cyber hazards and the GEIGER Education Eco9system" (Remmele, 2021, p. 4). The GEE approaches the human component by targeting multiple target groups, from typical employees with low cybersecurity responsibilities to designated personnel responsible for monitoring cyber security utilizing the GEIGER Toolbox.

Personal data for quality control and system improvement is crucial to the company's growth. Data must be adjusted to disguise the subject’s identity under confidentiality requirements.

Observe guidelines for obtaining personal data. Using the above factors, identities, data access, and dangers are classified. This loop should be conducted with each new access to personal data, even if distinct processes require a shared strategy for actions. In most circumstances, personal data protection is based on general purposes and basic information standards. In other words, the personal data protection approach will be common, but its implementation will be different. Data depersonalization destroys the link between a collection of characteristics and a personal data subject. Employers use technological monitoring to watch employees' work and read their emails.

Privacy means the right to be alone. It's a personal, philosophical right widely recognized.

**References**

Adnan, S. (2021). *Impact of employer monitoring on remote workers* (Doctoral dissertation,

Auckland University of Technology).

Ashton, L. (2022, January 28). *Data Breach Reporting: The Complete Guide*. Data Breach

Help. Retrieved September 22, 2022, from <https://www.data-breaches.co.uk/data-breach-protection-claims-and-compensation/reporting/>

Bajec, M., & Krisper, M. (2005). A methodology and tool support for managing business rules in organisations. *Information Systems*, *30*(6), 423–443. <https://doi.org/10.1016/j.is.2004.05.003>

Brassart Olsen, C. (2020). To track or not to track? employees’ data privacy in the age of Corporate Wellness, mobile health, and GDPR†. *International Data Privacy Law*, *10*(3), 236–252. <https://doi.org/10.1093/idpl/ipaa004>

Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: Causes, challenges, prevention, and Future Directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5). <https://doi.org/10.1002/widm.1211>

Dillon, T. W., Hamilton, A. J., Thomas, D. S., & Usry, M. L. (2008). The importance of communicating workplace privacy policies. *Employee Responsibilities and Rights Journal,* 20(2), 119-139.

De Capitani di Vimercat, S., FORESTI, S. A. R. A., Livraga, G., & Samarati, P. (2012). Data Privacy: Definitions and Techniques. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *20*(06), 793–817.

Hendrickx, F. (2022). Protection of workers’ personal data: General principles. *ILO Working Paper*. <https://doi.org/10.54394/vbkr9991>

Kaur, K., Gupta, I., & Singh, A. K. (2017). A comparative evaluation of data leakage/loss prevention systems (DLPS). *Computer Science & Information Technology (CS & IT)*. <https://doi.org/10.5121/csit.2017.71008>

Lulandala, E. E. (2020). Facebook data breach: A systematic review of its consequences on consumers’ behaviour towards advertising. *Strategic System Assurance and Business Analytics*, 45–68. <https://doi.org/10.1007/978-981-15-3647-2_5>

Friedman, B.A., Reed, L.J. Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-mail Use. *Employ Respons Rights J* 19, 75–83 (2007). <https://doi.org/10.1007/s10672-007-9035-1>

Miller, S., & Weckert, J. (2000). Privacy, the Workplace and the Internet. *Journal of Business Ethics,* 28(3), 255-265.

Mishra, J. M., & Crampton, S. M. (2021). Employee monitoring: privacy in the workplace? *SAM Advanced Management Journal*, *86*(2). <https://doi.org/10.52770/lhzu5765>

Moore, A. D. (2000). Employee monitoring and computer technology: Evaluative Surveillance V. Privacy. *Business Ethics Quarterly*, *10*(3), 697–709. <https://doi.org/10.2307/3857899>

Towns, D. M., & Cobb, L. M. (2012). Notes on: GPS technology; employee monitoring enters a new era. *Labor Law Journal*, *63*(3), 203.

Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. *Informing Science: The International Journal of an Emerging Transdiscipline*, *19*, 277–301. <https://doi.org/10.28945/3573>

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, *34*(6), 1247–1257. <https://doi.org/10.1016/j.clsr.2018.08.006>

Richard O. Mason Southern Methodist University, Mason, R. O., University, S. M., & Metrics, O. M. V. A. (1986, March 1). *Four ethical issues of the information age*. MIS Quarterly. Retrieved September 30, 2022, from <https://dl.acm.org/doi/10.2307/248873>

Remmele, B., & Peichl, J. (2021, August). Structuring a Cybersecurity Curriculum for Non-IT Employees of Micro-and Small Enterprises. *In The 16th International Conference on Availability, Reliability and Security* (pp. 1-7).

Shoshitaishvili, Y., Kruegel, C., & Vigna, G. (2015). Portrait of a privacy invasion. *Proceedings on Privacy Enhancing Technologies*, *2015*(1), 41–60. <https://doi.org/10.1515/popets-2015-0004>

von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers & Security*, *23*(4), 275–279. <https://doi.org/10.1016/j.cose.2004.01.013>

Wang, Y. (2022). Protection of employees’ personal information under Workplace Surveillance. *Beijing Law Review*, *13*(02), 350–364. <https://doi.org/10.4236/blr.2022.132023>

*What is employee safety and its importance & responsibilities?* ComplianceQuest QHSE Solutions. (2022, September 21). Retrieved September 30, 2022, from <https://www.compliancequest.com/employee-safety-importance-and-responsibilities/>