An Assessment of Some Ethical Challenges to Employee Privacy and Consumer Privacy in the Business World

Kumar Neeraj Sachdev
Associate Professor
Birla Institute of Technology
and Science (BITS), Pilani Campus
Pilani, Rajasthan, India.

Pritika Ramu
Student
Birla Institute of Technology
and Science (BITS), Pilani Campus
Pilani, Rajasthan, India.

Abstract

Privacy is essential to individuals as it gives them space to be themselves without judgement and discrimination. Employers collect information about employees, and ethical issues arise while handling their records, even though there are instances when it is justified. However, employers are responsible for maintaining employee privacy to ensure credibility and improve employee performance. The increased use of the Internet and the boom of big data analytics have raised concerns regarding employee privacy. Internet users, especially consumers, state that they value privacy but obtain much material gain in exchange for sharing personal information. We assess the contentious issues that arise in these areas to argue that protecting privacy is a moral imperative and requires ethical sensitivity and support of the legislation. For this purpose, we delve into ethical approaches and the principles of protecting online privacy. We come to the view that protecting privacy in the workplace requires a coordinated moral solution between many parties.

Keywords

Privacy, Employer-employee relationship, Employee privacy, Utilitarianism, Kantianism, Consumer privacy, and Big Data analysis.

1. Introduction

Privacy is a right to be left alone. It is essential for autonomy and the protection of human dignity. It serves as the foundation upon which many other human rights are built. Privacy enables us to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, thus allowing us to have control over ourselves. Privacy helps us to establish boundaries to limit who has access to our minds, bodies, places and things, as well as our communications and information. As employees desire privacy, but the mere fact that they have this desire does not make it valid to have a right. Both employers and employees have reasons to share information in the workplace, but contentious issues arise in practical situations. There are challenges in maintaining a balance between employer's requirements and expectations and employee privacy. We suggest the

application of moral arguments to overcome these challenges that can be classified into two categories to establish the value of privacy. One type of utilitarian argument appeals to consequences, and the second type is a Kantian argument that links privacy to being a person or having respect for persons. In continuation, we examine contentious issues regarding consumer privacy, mainly in the context of big data in the business world. Finally, we refer to specific principles of protecting online privacy to arrive at concluding remarks.

2. Privacy in the Workplace

Employers claim they are forced to monitor employees due to changing work nature (North, 1977, pp. 717-719). For example, the systems for executing financial transactions and transferring funds used by banks and securities firms have great potential for misuse and costly errors. As employers administer insurance plans and provide on-site health care, they are in a position to know about employees' medical conditions. Employers are increasingly concerned about the use of drugs by workers and the high cost of employee theft, including the stealing of trade secrets. Employers also claim to provide a safe workplace in which employees are free from the risk of being injured by intoxicated co-workers (Preston, 1998, pp. 12-18). Employers require tremendous amounts of important information for the hiring and placement of workers evaluating their performances. They also monitor "off-the-clock" activity to ensure their actions do not negatively influence them. Employee privacy concerns are regarding the information the employer may possess and how it is used. Whether the possession of such personal information is legitimate depends on the relationship between an employee and an employer. The core of this relationship is that employees are agents of their employer.

2.1 Justifying Monitoring of Employees

Employers argue that personal behaviour, even when it takes place away from work, can indirectly impact the ability of an employee to perform well on the job. They are concerned about the use of drugs by workers and randomly test for drug use to provide a safe workplace. Drug use occurrences away from the workplace during the employee's time still affects work performance and the workplace environment. Testing for drug use benefits not only the company but all employees.

The second argument is that what an employee does in her spare time can substantially increase the costs of doing business. The cost of providing insurance coverage has prompted some companies to take a more active role in monitoring the personal activities of their employees. Employee wellness

programs are a popular tool for helping companies to reduce the cost of providing health insurance by encouraging employees to lead healthier lives.

2.2 Privacy of Employee Records

Some of the issues that arise are related to the kind of information that is collected, the use to which the information is put, the persons within a company who have access to the report, the disclosure of the information to persons outside the company to gain the information, the steps taken to ensure the accuracy and completeness of the information, the access that employees have to information about themselves.

It is essential to justify a purpose to determine the exact scope of the right of privacy in employment (OpenStax, 2018). Although there is room for disagreement, it is essential to judge whether any given purpose is legitimate for a business, whether a certain kind of information is necessary for a business, and whether the information is being used for the intended purpose (Federal Trade Commission, 2020). For example, employers share the content of personnel files with lending agencies, subsequent employers, and other inquiring persons without the employees' consent. Even when there is a legitimate purpose that would justify these outsiders having the information, it can be argued that an employer has no right to provide it because the employer is justified in collecting and using information only for purposes connected with the employer-employee relationship. Use of certain means may violate an employee's right to privacy, even when the information gathered is of a kind that an employer is fully justified in possessing. Examples of impermissible means are polygraph testing and informal interviews. A major consideration in evaluating the means used to gather information is whether less intrusive means are available. In general, less intrusive means are morally preferable to those that are more intrusive. Since the information collected is going to affect significant personnel decisions such as hiring and firing, it is only fair that the information is as accurate and complete as possible and that employees have access to their personnel files so that they can challenge the contents or at least seek to protect themselves from adverse treatment based on the information in them. This can be viewed from the utilitarian calculation of benefit and harm and from the Kantian spirit of treating employees as ends rather than means. They are autonomous, rational and dignified human beings and hence should not be harmed and manipulated.

3. Utilitarian Arguments for Valuing Privacy

Mill argues for the maximization of individuals' happiness simply because individuals are capable of rationally calculating the happiness of all human beings, especially the concerned individuals in a situation in an impartial and objective manner (Mill, 1993). On the contrary, "a great harm is done to individuals when inaccurate or incomplete information is collected by an employer is used as the basis for making important personnel decisions, for example, groundless accusations or record of arrest without conviction in their personnel records when employees are unable to examine their files (Boatright, et al, 2018, pp. 155-156)." Employees' lives get disrupted by groundless accusations in their personnel records. The harm is more likely to occur when employees cannot examine their files and challenge the information (or misinformation) in them (Ibid).

However, there is an unproven assumption in the argument that on a utilitarian calculation more harm than benefit will occur if such personnel practices are adopted. Still again on a utilitarian calculation, such personnel practices have to be examined whether on balance they produce more benefits for both employers and employees. This unproven assumption in the argument may be posing some challenges to the utilitarian defence of privacy. Still, on an advanced level of utilitarian argument, it is contended that some amount of privacy is necessary for getting the satisfaction of performing a job. In the case of monitoring and surveillance in the workplace, for example, this satisfaction gets declined. (Ibid.)

Interestingly, this utilitarian argument touches on the Kantian idea of a sense of dignity and self-worth of employees when it says privacy invasion sends a wrong signal to employees that they are not trusted and respected as human beings, which affects their sense of satisfaction. We look into the Kantian flavour of ethical arguments more directly.

4. Kantian Arguments for Valuing Privacy

Kantians argue that invading a person's privacy violates the principle of respect for persons and prevents a person from making a rational choice as an autonomous being (Kant, 2012; Boatright, et al, 2018, pp. 157). It is morally objectionable to be observed unknowingly through a hidden camera or have personal information in a data bank; because a person loses control over how they appear to others. If people form incomplete or misleading impressions of a person that they cannot correct, then he is denied the possibility of autonomous or self-directed activity, which is a characteristic of being human. Hence, it is claimed that invasions of privacy diminish an essential condition of being human (Ibid, pp. 148-178).

Furthermore, privacy provides a rational context to love, friendship, and respect because these words speak about intimate relations, which are primarily based upon the intimate sharing of personal information. Similarly, trust as a relation of mutual expectation that people will behave in a certain manner cannot exist, for example, outstation work assignments or even travel expenses incurred during such an assignment, if there is monitoring or surveillance.

The issue of loss of privacy of employees may further be assessed in a larger domain of big data analysis, which affects not only employees but consumers of goods and services in general.

5. Big Data Analysis

Big data analysis refers to a process that merges large sets of consumer and other data with the help of information technology in an effort to make predictions, especially about human behaviour. Everyday activities such as shopping online, using a fitness app on a mobile device, or any activity on social media create information trails that are extremely valuable to marketing firms. With this information, companies have improved their ability to identify consumers, understand their needs, and anticipate their purchasing behaviour. Privacy experts scrutinize the ethical issues raised by the activities of the companies that specialize in data collection and analysis. Big data analytics has been growing due to the following two reasons:

First, the Internet provides a platform on which almost every individual decision can be recorded and archived. As the internet gets more comfortable to access, more data is collected. "The pace of the internet, accessibility of social media platforms, and its availability over portable digital devices has completely thinned the circulation period of any kind of information written or shared through audio, video or written modes could have a positive or negative contagious impact in a fraction of time." (Arun Kumar and Kiran Saroj, p. 106)

Second, an increased ability to analyse the growing amount of data provides a greater opportunity to discover behavioural patterns to make predictions about future wants and actions. It reflects a shift in the marketing matrix from the 4Ps namely product, price, promotion, and placement to 4Cs which include "consumer wants and needs, the cost to satisfy, convenience to buy, and communication (Ibid., pp. 106-107)." The reason is that the rise of complex and sophisticated algorithms with the use of machine learning and artificial intelligence has made this easier.

5.1 Ethical Issues with Big Data

The most common crime over the internet is identity theft. Identity theft can compromise everyday activities and undermine one's reputation, privately and

professionally. Concerns over consumer privacy have been heightened in recent years not only by the increased use of the Internet and data analysis. The criticisms of big data analysis include the lack of transparency of data analysis, the business practices of data aggregators, and the loss of privacy by consumers (Tene, 2019). Three reasons may be put forward to clarify the ethical issues with big data:

Lack of Awareness: The collection and distribution of big data occur without much legal oversight. The technology used to mine existing data is used without the knowledge of Internet users. This lack of knowledge means that individuals cannot take steps to protect their personal information and prevent it from being collected or distributed. More importantly, consumers have little knowledge of how their personal information is analysed and used.

The Difficulty of Protection: Even if consumers were aware of the collection, analysis, and use of big data, they could not easily use this knowledge to protect their privacy. Data aggregators share and sell data among themselves and obtain information from ad networks with which they are affiliated. Ad networks, in turn, use data compiled by aggregators to target advertisements across websites and mobile devices. This constant free flow of data makes it difficult for users to protect themselves from all the aggregators.

Loss of Privacy: The aggregators collect discrete data from different parts of the internet and create a whole picture of an individual's identity, covering factors from every dimension of life. This could possibly be a false identity for other people to know. The whole identity of an individual reveals much more than the individual pieces from which it is made and thus constitutes a more significant invasion of privacy. "Indeed organizations that take advantage of the business benefits that big data promises, but fail to appropriately reconcile these concerns, risk repercussions that could cause serious detriment to their reputation, capabilities, and overall competitive advantage (Burkhardt et al, 2022)." We report five principles to address these ethical issues with big data (Boatright, et al, 2018, pp. 171-172).

6. Principles of Protecting Privacy

The principles of protecting privacy help to protect internet privacy even though certain issues arise in their interpretation and implementation (Boatright, et al, 2018, p. 172; Federal Trade Commission, 2020).

Notice/Awareness: The identity of the collecting party and the use of the information collected should be disclosed. The privacy policy should be

prominently displayed and easily understood. They should provide details about the party with whom they share the data.

Choice/Consent: Provide a mechanism for choosing whether to allow information to be collected. One could choose to permit the collection of some information (e.g., name and address) but no other (e.g., medical information), or one could consent to some uses of information (e.g., to select banner ads) but not others (e.g., sharing data to a third party).

Access/Participation: Allow consumers access to the information collected about them and to verify the accuracy of the information.

Integrity/Security: Inform users of the steps taken to protect against the alteration, misappropriation, or destruction of data and of the action that will be taken in the event of a breach of security. Also, maintain information so that it is accurate and up-to-date.

Enforcement/Redress: Companies should follow responsible information practices and face the consequences if they fail to do so. One way to ensure enforcement and redress is by contracting with an organisation that monitors and certifies the information practices of websites.

These principles are of help to protect the cause of internet privacy if all parties mainly internet companies abide by the moral need to strictly interpret them and deploy the appropriate means to implement them (Ibid.). On various occasions, a self-centric interpretation of principles of protecting the privacy and the absence of socio-legal intervention require a value-oriented intervention on behalf of the internet user as a creator or a user. An internet user is also expected to own moral responsibility for his role in sharing information or communication through various channels. The internet does not spy on a user's activity like a hidden camera, it can be considered a public arena, and the user voluntarily loses privacy to gain the benefits of using the internet.

7. Conclusion

People value privacy and ethical theories back the claim of the need for privacy protection. The problems faced by employees, consumers, and Internet users are similar, as are the solutions. More than 120 countries have data protection laws to prevent the misuse of information and to ensure privacy. The technologies that threaten privacy have also brought us many benefits. Finding the right means to protect privacy is a great challenge to businesses that must meet employee and consumer expectations as they use new technologies. More than many other ethical problems in business, protecting privacy requires a coordinated solution involving many parties. Until a solution is found, developing and implementing privacy policies will remain a challenge for businesses and society. It is possible to an extent to meet this challenge if all parties act in such a morally responsible

manner that their claims of each other are truthful and compassionate. The purpose of the business, after all, is to serve the public by providing desired and desirable products and services and by not harming the community and its citizens (Solomon 2003: 361)."

8. References

1. Boatright, J. R., Smith, J. D., & Patra, B. P. (2018). "Privacy" in Ethics and the Conduct of Business, *Pearson*, pp 148-178
2. Burkhardt, Gary, Boy, Frederic, Doneddu, Daniele and Hajli, Nick (2022). Privacy Behaviour: A Model for Online Informed Consent. *Journal of Business Ethics https://doi.org/10.1007/s10551-022-05202-1*
3. Federal Trade Commission (2020, July 16). *Protecting Personal Information: A Guide for Business.* Retrieved from *https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business*
4. Kant, Immanuel (2012). *The Moral Law.* London and New York: Routledge Classics.
5. Kumar, Arun and Saroj, Kiran (2020, December). Impact of Customer Review on Social Media Marketing Strategies, *International Journal of Research in Business Studies*, Vol. 5 (2), pp. 105-114.
6. Mill, John Stuart (1993). *On Liberty and Utilitarianism.* New York, USA: Bantam Classics.
7. North, John C. (1977). *Responsibility of Employers for the Actions of Their Employees: The Negligent Hiring Theory of Liability*, 53 (3), pp 717-730. Retrieved from *https://scholarship.kentlaw.iit.edu/cklawreview/vol53/iss3/8*
8. OpenStax (2018, September 20). *Privacy in the Workplace*. Retrieved from *https://opentextbc.ca/businessethicsopenstax/chapter/privacy-in-the-workplace/*
9. Paul, R. (2019, October 31). *Privacy as a Utilitarian Value*. Retrieved from *https://www.lawfareblog.com/privacy-utilitarian-value*
10. Preston, D. S. (1998, December 01). *Business Ethics and Privacy in the Workplace*, 28 (4), pp 12-18. Retrieved from *https://dl.acm.org/doi/abs/10.1145/308364.308367*
11. Solomon, Robert C. (1993). *Business Ethics: A Companion to Ethics*. Edited by Peter Singer. Oxford, UK: Blackwell Publishers, pp. 354-365.
12. Tene, Omer and Polonetsky, Jules (2019, April 13). *Privacy in the Age of Big Data*. Stanford Law Review. Retrieved from *https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/*