Ethical or Not: Monitoring Employees' Online Activity by Companies

Course Name

July 15, 2025

Ethical or Not: Monitoring Employees' Online Activity by Companies

In today's society, the distinction between personal privacy and professional accountability is becoming narrower every day. One issue that has generated a lot of heated debate in workplaces across the country is the company's monitoring, or surveillance, of employees' online activities. Even though employers' surveillance—i.e., monitoring online activity—seems productive to employers (for a variety of reasons, including productivity, cybersecurity, and compliance with laws), employees view it as an invasion of their privacy. As it becomes more common for people to work remotely and communicate via online media, the ethical consequences of natural surveillance have become more complicated. Decisions regarding monitoring are ethically dependent on many factors including how the company monitors (the means), and the rationale for monitoring (the ends), while also considering employee autonomy and trust (Smith & Jones, 2022). The purpose of this paper is to explore the justification for monitoring, as well as the ethical implications of monitoring.

Justifications for Monitoring Employee Online Activity

There are a number of valid reasons why employers may view online behavior. Among the most quoted reasons is the protection of organizational resources and assuring their productivity. Distractions (digital distractions) may reduce performance drastically; so, monitoring the actions on the websites or apps may assist the employer to detect inefficiencies (Brown, 2021). Also, in most industries, strict rules are to be followed. To illustrate, sensitive data in the context of financial institutions or healthcare providers have to be secured according to laws such as HIPAA or GDPR. Breach or unauthorized access can be detected through monitoring, which would have otherwise not been discovered.

The other rationale corresponds to cybersecurity. As the number of phishing, malware, and insider threats grows, businesses will have to take initiative in protecting themselves against cyber risks. It could keep an eye on threats in real time and monitor software helps avoid data breaches which can be quite expensive. As an example, it was stated by Deloitte (2023) that 48 percent of data breaches in 2022 were caused by negligence or using access by employees, which further supports the idea of strict monitoring. Furthermore, teleworking has also widened the threat scenario with unsecure networks and personal devices raising the exposure. In this regard, the concept of monitoring is offered as the corporate self-protection instead of distrust toward the employees.

From a legal point of view, many countries permit the reasonable monitoring of workplace communication as long as employees have been informed. Organizations typically have monitoring policies included in employment contracts or in handbooks. This protects the organization legally and assists with compliance in general while providing transparency. Additionally, if the organization responsibly engages in monitoring while disclosing the monitoring activity, it can be argued that the organization is not actually conducting unethical monitoring but rather using monitoring as a risk management strategy (Khan & Roberts, 2021).

Ethical Concerns and Employee Rights

In spite of such justifications, critics believe that monitoring is a violation of the crucial rights of autonomy, dignity and privacy. Employers may overstep ethical lines when they keep an eye on the emails, keystrokes, or even social media use and such monitoring may be a cross over provided it is not accompanied by an informed consent by the employee or workers. The suspicion that one is always under someone will trigger psychological strain and low morale and

create an environment of suspicion (Lopez & Greene, 2022). This can cause disengagement that, in fact, works against the productivity employers want to preserve.

There is as well the risk of unequal or selective surveillance. When other groups are monitored to a greater extent than others, by design or accident, it can create allegations of discrimination or unfairness in the workplace. Ethical issues are more acute when they relate to spillage into personal time, like tracking of lunch time or after hours activities, and in cases where there is dual-purpose equipment used by employees. Ahmed and Lin (2024) stated that 62 percent of employees hired in hybrid occupations raised claims about intrusive surveillance, and they demanded a clear distinction between professional and personal life.

In addition, surveillance may affect innovation and creativity in a wrong way. Workers who feel spied on all the time will hesitate to take risks or even offer innovative ideas as they perceive that every move is being judged. Trust and psychological safety are the pillars of ethical workplace cultures that are eroded by blanket surveillance. Transparency is important, otherwise even with the transparency, the power imbalance between the employer and the employee makes the consent a challenge on behalf of the employee. Ethical monitoring needs to have well-established boundaries, data minimization approach, and the option to appeal or opt-out where possible among employees.

Conclusion

The ethical considerations around employee monitoring of online behavior rely on the balance between the needs of the organization and the rights of individuals. There are plenty of arguments for monitoring, particularly in regard to productivity, cybersecurity, and compliance with regulations; all of these must be balanced with privacy concerns and the possibility of

abuse. Ethical monitoring must be transparent, proportionate, and fair. Organizations should establish policies that honour the dignity of the employee, and trust them rather than be suspicious of them. It is not the act of monitoring that is unethical, but the way, why, and how much monitoring is done.

References

Ahmed, F., & Lin, J. (2024). *Employee perceptions of digital surveillance in remote workplaces: Ethics and boundaries*. Journal of Business Ethics, 177(2), 311–329. https://doi.org/10.1007/s10551-023-05317-w

Brown, C. (2021). *Monitoring productivity or invading privacy? A legal and ethical analysis of employee surveillance*. Harvard Business Law Review, 11(2), 45–67.

Deloitte. (2023). *Global cyber report 2023: Rethinking digital risk*. https://www2.deloitte.com/global-cyber-report-2023

Khan, R., & Roberts, S. (2021). *Balancing corporate needs and individual rights: Ethics in workplace surveillance*. Business and Society Review, 126(4), 567–586. https://doi.org/10.1111/basr.12243

Lopez, D., & Greene, M. (2022). *The psychological toll of workplace monitoring*. Industrial and Organizational Psychology Perspectives, 15(1), 88–102.

Smith, A., & Jones, T. (2022). *Digital ethics and employee autonomy: Revisiting surveillance in the modern workplace*. Ethics and Information Technology, 24(3), 425–440. https://doi.org/10.1007/s10676-021-09621-9