International Academic Institute for Science and Technology

International Academic Journal of Organizational Behavior and Human Resource Management
Vol. 13, No. 2, 2026, pp. 9-13.

ISSN 2454-2210

International Academic Journal of Organizational Behavior and Human Resource Management

www.iaiest.com

Employee Data Privacy and Consent in Workplace Surveillance Systems

Amir Hosseini [a*], Sara Rahimi [b]

[a*] *Iranian Institute for Emerging Science Research, Tehran, Iran.*
[b] *Iranian Institute for Emerging Science Research, Tehran, Iran.*

Abstract

Employee surveillance has evolved from an occasional tool of managerial control to an extensive surveillance apparatus in today's employment relation. The contemporary employers monitor keystrokes, computer usage, locations, communication channels, physiological responses, and emotional displays, and thus collect information that is highly personal, constant, and often gathered beyond the literal confines of the workplace. The present paper considers the conflict between data privacy of employees and mechanisms of consent typically used to justify such monitoring. It is suggested that consent, as it is designed in both the law and the management practices today, is inherently incapable of fulfilling its legitimizing role in the employment relation due to the asymmetry of powers between the employer and the employee. Following the assessment of the technological landscape of surveillance systems at work, the paper examines the responses in legal doctrine to workplace surveillance from the European Union and the United States, which include GDPR, the EU Artificial Intelligence Act, the European Convention on Human Rights, a collection of US state monitoring laws, and collective bargaining on algorithmic governance. Finally, the paper examines empirical research on the effects of surveillance on trust, stress, satisfaction, and performance. In conclusion, the paper suggests a governance architecture that does away with consent as a key mechanism of legitimacy and substitutes it with necessity, proportionality, transparency, workers' voice, and accountability.

Keywords: Workplace Surveillance, Employee Data Privacy, Consent Mechanisms, Electronic Performance Monitoring (EPM), Bossware, Power Asymmetry.

DOI: 10.71086/IAJOBHRM/V13I2/IAJOBHRM1307
Received: 04 March 2026/Revised: 14 April 2026/Accepted: 22 May 2026/Published: 30 June 2026

Introduction

Observation has always been part of the employment relationship. What is different in the current age is not the presence of surveillance but its level of granularity, consistency, and analysis. Digitalization has made possible the monitoring not only of work but also of the cognitive, affective, and behavioral processes of the employee. This can be done through the tracking of movements, web activity, and heart rate and blood pressure via common technology that is integrated into common consumer products. The advent of remote and hybrid work has further contributed to this process, because the gap between the workplace and the home has narrowed down, thus eliminating the distinction between work and private life. Almost 80% of US employers use electronic performance monitoring, and the market of employee surveillance software, commonly called bossware, has grown fast, including such functions as keystroke logging, location tracking, browser monitoring, and webcam activation.

The paper argues its case in the following four sections. Firstly, it discusses the theoretical basis of the concepts of surveillance, privacy, and consent and differentiates between consent and other related terms such as notice, acknowledgment, and acquiescence. Secondly, it describes the technology behind modern workplace surveillance, such as electronic performance monitoring and bossware, emotion detection, biometrics, and wearable technologies. Thirdly, it outlines the legal frameworks within which these practices take place in the European Union and the United States and the potential emergence of the collective worker voice. Fourthly, it reviews the empirical literature on the outcomes of surveillance and suggests a comprehensive governance model for management.

The key thesis here is that those organizations using consent as the main form of legitimacy are both legally and managerial failures. Legally, because consent is legally fragile in an employment situation; and managerially, because it has been empirically proven that when surveillance is seen as invasive, it causes stress and lowers performance levels.

Conceptual Foundations: Surveillance, Privacy, and the Problematic Status of Consent

Defining Workplace Surveillance

EPM is defined as the application of technological techniques to monitor, measure and analyze information which directly or indirectly affects job performance. EPM is a deliberately broad term because surveillance itself is a broad concept which includes monitoring data regarding the work and regarding workers, logging communication, tracking physical movement and presence, and even inferring states and dispositions based on behavior and physiology. In a recent systematic review, workplace surveillance is described as a multi-dimensional organizational practice whose impact is driven by the structure of the surveillance as well as how employees perceive the surveillance (Kayas, 2023). This distinction is important because an organization may think that it has a system that works well in terms of not being harmful to the people, but the important variable would be what employees perceive from it. The idea of bossware helps understand the modern surveillance practice in greater detail. Such technologies include devices and software ranging from email and keystroke tracking to constant monitoring, and their application has spread despite a lack of any federal legislation in the U.S. that could protect workers from it (Hewitt, 2023). One analogy draws upon Foucault's understanding of power and technology in order to describe modern bossware as an "e-panopticon," a structure in which the possibility of constant surveillance regulates people's conduct even if no real surveillance takes place. This panoptic paradigm is significant for management theory in that it provides a mechanism by which surveillance takes place without monitoring at all.

Privacy in the Workplace: a Contested and Contextual Interest

Privacy in employment does not comprise a single legal or moral interest, but it is made up of several interests relating to information control, autonomy, bodily integrity, and the distinction between employment and personal spheres. According to the case of Bărbulescu v. Romania, the European Court of Human Rights acknowledged that surveillance amounts to interference with one’s right to respect for private life as provided for in Article 8 of the European Convention on Human Rights. In this case, the court found that the Romanian justice system had failed to strike a balance between the right to surveillance and the right to privacy. The rationale used by the Grand Chamber is telling in its own way as well: the Grand Chamber stated that “the presence of a reasonable expectation of privacy is a significant but not necessarily conclusive factor” in establishing if Article 8 is engaged and that there were no indications that the worker was aware of the details of the monitoring before it took place (Atkinson, 2018). Scholars have noted that the reasonable-expectation approach per se makes the concept of workplace privacy weak, as it ignores the damage done by overt surveillance.

The final conceptual innovation revolves around the extent of the private interest involved. Research conducted on the subject of emotion artificial intelligence in the workplace discovered that the participants regarded the use of emotion AI as a significant intrusion into privacy in relation to the private and sensitive emotional data of workers, the ability to be used to force conformity to standards of emotional labor, and the use of emotional labor by workers themselves as a tool for preserving emotional privacy; the authors suggest defining the "right to emotional privacy" (Roemmich et al., 2023) . A related discussion asserts that affective privacy is a civil right, expanding on the concept of intimate privacy in relation to identity, body, health, and interpersonal relations.

The Anatomy of Consent

Consent seems to be a simple term but is rather difficult to analyze. In the employment monitoring scholarship, consent is used to refer to an array of agreements that vary tremendously in terms of how much protection they offer. On one end of the spectrum stands consent that is strong and as prescribed by the European law, which would mean that it must ensure that an employee could refuse to agree to monitoring without any adverse effect on his/her job—meaning not only dismissal but also the change in his/her job terms and conditions that would be viewed negatively. On the opposite end of the spectrum stands consent that is constructive in nature, which would enable the employer to say that the employees gave consent knowing well that they should have known about monitoring or because of certain laws like the property right of the employer to the equipment issued by him/her. The key point is that the majority of consent mechanisms used by employers fall towards the less powerful end of the spectrum but claim legitimacy as though falling on the more powerful end. A simple statement within an employee handbook that states that monitoring will be done by the employer is not consent in any moral or legal sense; rather, it is just a way of informing the employee of a fact which he or she cannot refuse.

The Technological Landscape of Workplace Surveillance

Electronic Performance Monitoring and its Variegated Intensity

Electronic Performance Monitoring now comes in many varieties, each of which varies greatly in terms of invasiveness. Studies conducted to analyze the reactions of employees to such monitoring have shown that the invasiveness increases as the type of monitoring moves from screen time monitoring, to screen activity monitoring through screenshots, and further to monitoring of social interactions through face reading. It is very significant to make this distinction as it proves that there is not just a binary state of being invasive, but there exists a spectrum of it, as perceived by employees. Drivers for adoption are known quite well. With employee monitoring software being available and relatively inexpensive on the open market, organizations are able to get strong surveillance tools like keystroke logging, location tracking, and browser monitoring; the most widespread industries where bossware is employed and the reasons why companies use it are revealed in the survey conducted in Canada, and they include COVID-19, productivity and efficiency, cybersecurity, and health and wellness, along with popular features such as time tracking, website tracking, and keystroke logging. The factors influencing bossware development are seen by researchers as the newness of the technology and quick shift to remote working amid the pandemic, as well as the business-friendly context when data privacy laws have very narrow application in the labor sphere and employers have great leeway in collecting and owning the collected data.

Biometric Systems

Biometrics, including fingerprints, facial recognition, and eye scans, have become increasingly common in workplaces for authentication purposes, access control, and timesheet management. Since there is no legislation at the federal level that regulates employers' gathering of biometric data, employers can force the use of biometric-enabled processes as a condition of employment; biometric data is not replicable and is usually connected to personal and financial accounts, and when employers gather biometric data, they generally depend on third parties for information technology services and storage, making the process vulnerable to data breach, malfunction, and third-party interference. "Use it or lose it" is one of the most common aspects of biometric enrollment regardless of whether it is for timesheet management, authentication, or security purposes (Holland & Tham, 2022). The Australian case where termination of employment based on lack of consent to biometric data gathering was reversed via the legislation demonstrates not only the growing push to collect biometric data but also the arbitrary character of legal protection and provides advice on collecting, storing, and managing biometric data. International studies draw the same conclusions: in Ecuador, biometric data increases the efficiency and safety of processes but also creates ethical and legal problems because of the lack of consent mechanisms and power imbalance threatening basic human rights; generally, biometric technologies may lead to serious interference into privacy and endanger the dignity of persons, especially in workplace access control to private data and territories (Collins & Marassi, 2021).

Why Consent Fails in the Employment Relationship

Doctrinal Invalidation

Perhaps the clearest indication of consent's limitations in the judicial and regulatory arena is in the case of the GDPR. In light of the introduction of this regulation, the possibility of obtaining prima facie consent to the processing of data in the employment context seems to be impossible in view of the great disparities of power that are at the heart of the employment relation; the GDPR itself makes explicit reference to the fact that consent in the employment context will not be valid as not being "freely given." Where the processing of data relies on consent as its justification, the Regulation stipulates that where there is a "clear imbalance" between the data subject and the controller, consent will not be valid, and the employment relationship will be one example of such an imbalance; in the employment context, data collection and processing must be justified by the requirements of the employment relation or the employer (Abraha, 2022). This means that there is an implication of this principle for the design of surveillance system. If consent is not possible to be used legally, then the employer will have to find a legal basis for processing such as "contract performance" or "legitimate interests of the employer". It is a much higher burden than just getting the signature. In case where processing of the employee's personal data is required, the GDPR requires the employer to mitigate the adverse impact on the employees such as not monitoring the employees in certain locations or not continuously but in sampling way. However, some regimes take it a step further and render consent completely ineffective in relation to certain types of employment processing. For instance, in the Finnish Act on Protection of Privacy in Working Life, the concept of necessity is used as a prerequisite for processing any employee personal information, which is necessary because the personal information needs to be directly relevant to the employment, and more importantly, this element is not qualified by consent in that the information processing will be unlawful if there is no such purpose even if the employee consents.

The structural critique

The doctrinal approach, however, contains a larger critique of structure. As a result of the unequal position that both the employee and the employer usually occupy in negotiations, the problem of securing consent becomes questionable. This issue was put forward by the European Data Protection Supervisor who asked the simple yet important question of whether any consent exists within the relationship between the employer and the employee. The practical effect of this situation becomes that of the procedure being used only for show (Yusifli, 2024). There is also a second, less obvious issue: the consent process is structurally flawed, both in the way in which it is granted and in the way in which it serves as a mechanism of governance. Information is gathered for one purpose and then used for another. Most of the information collected from employees while they do their job or simply live their lives gains its potency in the way in which it becomes aggregated with other information; companies will almost certainly be able to claim that this information falls into the category of information that a company collects as part of its normal operations, and the courts have shown a fair amount of deference to claims by companies regarding business interests (Doellgast et al., 2023).

Consequences of Surveillance: What the Evidence Shows

Well-Being, Attitudes, and Performance

A significant amount of empirical research exists about the effects of surveillance, and much of it is in the form of meta-analysis. One such study examined 70 independent samples and 233 effect sizes to find that electronic monitoring weakly reduces job satisfaction ($r = -0.10$) and increases stress ($r = .11$). This confirms the theory that surveillance has a negative impact on the psychological and professional well-being of employees; moderator analyses show that performance targets and feedback increase this negative impact. But more importantly, the same study revealed that there is no link between electronic monitoring and performance ($r = -0.01$) and a weak positive link with counterproductive work behavior ($r = 0.09$) (Siegel et al., 2022).

A survey conducted with 1,119 participants revealed that electronic performance monitoring perception highly correlates with increased privacy invasion, low organizational trust, higher individual stress, and poor individual performance; perception of privacy invasion correlated with low organizational trust, and low organizational trust was associated with higher individual stress (Kalischko & Riedl, 2024). A survey conducted with 3,508 Canadians using the structural equation modeling method revealed that the perception of surveillance is indirectly correlated with the increase in psychological distress and lower job satisfaction because of stress proliferation; these negative effects were explained by the relationship of surveillance with three secondary work stressors, which include job pressure, autonomy reduction, and privacy violation (Glavin et al., 2024). Previous research demonstrated similar outcomes including stress and mistrust increase, job and work quality reduction, and customer service reduction with health

issues like stress, high tension, headaches, severe anxiety, depression, anger, tiredness, and musculoskeletal disorders cited as responses to workplace surveillance, which can result in absenteeism, turnover, and lower productivity.

Reactance and the Privacy Calculus

However, necessity and invasiveness perceptions are interrelated. Thus, studies of monitoring types reported high adherence to the social norm against electronic monitoring, implying the existence of strong resistance to electronic monitoring, and found invasiveness, which exceeded screen time monitoring, to be highly privacy-invasive and relatively reactance-provoking. Additionally, awareness of rights is poor. As a result, two-study research reported that employees felt certain about the understanding of monitoring terminology but found themselves incapable of providing adequate definitions of those terms, that awareness of the existence of any legal protection differed by industry and position and was quite low and uncertain, and that participants found bossware unnecessary. The lack of understanding of the terminology of monitoring and legal protection makes employees even less aware of monitoring technologies used in their places of work (Bunwaree et al., 2025).

Conclusion

The protection of employee privacy in workplace surveillance systems via consent is not feasible. In employment relationships, the inherent imbalance of power makes voluntary consent impossible, an observation borne out by both EU and US laws. However, organizations still use consent tools such as acknowledgement sheets, handbooks, and enrollments in the belief that consent legitimized them, while doing neither legally nor managerially. They do nothing legally as the doctrinal foundations of the unavailability of consent in employment cases have been clearly laid out, and the criteria for testing consent have evolved to include necessity, proportionality, and business justification. At the managerial level, it does nothing either as the empirical data show that surveillance activities that employees perceive as intrusive lead to reactance, distrust, increased stress, and lowered job satisfaction without enhancing productivity.

References

Kayas, O. G. (2023). Workplace surveillance: A systematic review, integrative framework, and research agenda. *Journal of Business Research*, *168*, 114212. https://doi.org/10.1016/j.jbusres.2023.114212

Hewitt, B. (2023). Panoptic employment. *Science and Technology Law Review, 24*(2), 349–378. https://doi.org/10.52214/stlr.v24i2.11631

Atkinson, J. (2018). Workplace monitoring and the right to private life at work. *The Modern Law Review*, *81*(4), 688-700. https://doi.org/10.1016/j.jbusres.2023.114212

Roemmich, K., Schaub, F., & Andalibi, N. (2023, April). Emotion AI at work: Implications for workplace surveillance, emotional labor, and emotional privacy. In *Proceedings of the 2023 CHI conference on human factors in computing systems* (pp. 1-20). https://doi.org/10.1145/3544548.3580950

Holland, P., & Tham, T. L. (2022). Workplace biometrics: Protecting employee privacy one fingerprint at a time. *Economic and Industrial Democracy*, *43*(2), 501-515. https://doi.org/10.1177/0143831X20917453

Collins, P., & Marassi, S. (2021). Is that lawful? Data privacy and fitness trackers in the workplace. *International Journal of Comparative Labour Law and Industrial Relations*, *37*(1). https://doi.org/10.54648/ijcl2021003

Abraha, H. H. (2022). A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace. *International Data Privacy Law*, *12*(4), 276-296. https://doi.org/10.1093/idpl/ipac015

Yusifli, Z. (2024). European Union: The 'bouncing ball' effect of the EU Artificial Intelligence Act on employment relations. *Journal of AI Law and Regulation, 1*(2), 228–232. https://doi.org/10.21552/aire/2024/2/9

Doellgast, V., Wagner, I., & O'Brady, S. (2023). Negotiating limits on algorithmic management in digitalised services: cases from Germany and Norway. *Transfer: European Review of Labour and Research*, *29*(1), 105-120. https://doi.org/10.1177/10242589221143044

Siegel, R., König, C. J., & Lazar, V. (2022). The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior: A meta-analysis. *Computers in Human Behavior Reports*, *8*, 100227. https://doi.org/10.1016/j.chbr.2022.100227

Kalischko, T., & Riedl, R. (2024). On the consequences of electronic performance monitoring in organizations: theory and evidence. *Digital Transformation and Society*, *3*(1), 50-79. https://doi.org/10.1108/DTS-10-2022-0054

Glavin, P., Bierman, A., & Schieman, S. (2024). Private eyes, they see your every move: Workplace surveillance and worker well-being. *Social Currents*, *11*(4), 327-345. https://doi.org/10.1177/23294965241228874

Bunwaree, T. S., Stawarz, K., Collins, P., & Gould, S. J. (2025, April). Boss is aWare—Are you? Employee comprehension and legal awareness of workplace monitoring. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (pp. 1-19). https://doi.org/10.1145/3706598.3713651