EMPLOYEE PRIVACY IN THE AGE OF AI MONITORING

ANWER ADEM, ELIZABETH MITCHELL, & DAVID PONTIOUS

The rapid expansion of artificial intelligence ("AI") has transformed both the scope and intensity of workplace monitoring. Employers increasingly rely on AI-enabled surveillance systems to deter misconduct, evaluate productivity, and enhance workplace safety by continuously collecting and analyzing behavioral, biometric, and location-based data.[1] These systems are recalibrating the balance between managerial oversight and employee privacy by transforming discrete acts of supervision into persistent, data-driven observation.[2] By replacing discrete supervision with persistent, data-driven observation, AI surveillance reshapes the balance between managerial oversight and employee privacy, particularly in remote and hybrid work environments where work and personal lives increasingly overlap.

Existing United States legal frameworks provide fragmented and insufficient protection against AI-driven workplace surveillance. In the absence of federal laws particular to AI, courts rely on contextual standards such as reasonableness, notice, and expectations of privacy—permitting legitimate monitoring while scrutinizing practices that become continuous, covert, or disproportionate. AI-enabled surveillance strains this framework, revealing the need for clearer disclosure, limits on off-hours monitoring, and stronger governance of employee data.[3]

BACKGROUND

I. EMPLOYEE SURVEILLANCE TOOLS

AI-enabled workplace surveillance encompasses a wide range of technologies, including phone calls, email and internet use, keystroke logging, screen-capture software, GPS tracking, facial recognition, and behavioral analytics.[4] Employers use these tools to measure productivity, enforce compliance, and mitigate security risks.[5] Unlike conventional workplace supervision, AI monitoring operates continuously and often without direct employee awareness, increasing the likelihood of intrusion into private life.[6]

Beyond informational privacy concerns, persistent surveillance may exert psychological pressure that alters employee behavior, discourages creativity, and undermines job satisfaction. The breadth and opacity of these systems amplify their impact, particularly when monitoring extends beyond work hours or physical workplaces.

---

[1] FED. TRADE COMM'N, REMARKS OF BENJAMIN WISEMAN AT THE HARVARD JOURNAL OF LAW & TECHNOLOGY ON WORKER SURVEILLANCE AND AI 2–3 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Jolt-2-8-24-final.pdf.

[2] Sarah Krouse, *The New Ways Your Boss Is Spying on You*, WALL ST. J. (July 19, 2019, at 05:30 ET), https://www.wsj.com/articles/the-new-ways-your-boss-is-spying-on-you-11563528604.

[3] *Id.*

[4] Danielle Abril & Drew Harwell, *Keystroke Tracking, Screenshots, and Facial Recognition: The Boss May Be Watching Long After the Pandemic Ends*, WASH. POST. (Sep. 24, 2021), https://www.washingtonpost.com/technology/2021/09/24/remote-work-from-home-surveillance/.

[5] *Id.*

[6] *Id.*

II. STATUTORY FRAMEWORK

Employee privacy rights in the United States arise from a combination of federal statutes, state law, and common-law doctrines, rather than from a unified regulatory scheme. As a result, courts resolve workplace surveillance disputes by applying general privacy principles developed for earlier technologies, not statutory limits tailored to AI-enabled monitoring.[7]

Federal statutes impose only limited constraints. The Electronic Communications Privacy Act[8] ("ECPA") restricts the interception of wire, oral, and electronic communications, including those via telephone, email, and the internet. Broad statutory exceptions, however, permit employers to monitor communications conducted on employer-owned devices or systems and communications intercepted in the ordinary course of business.[9] These exceptions substantially narrow employee protections and leave many contemporary surveillance practices—particularly AI-driven monitoring—outside meaningful federal regulation. In the absence of legislative clarity, courts have assumed primary responsibility for defining the permissible scope of workplace surveillance.

DEVELOPING CASE LAW

Judicial treatment of workplace surveillance applies a context-specific reasonableness framework rather than categorical limits. Courts evaluate monitoring by balancing employee privacy interests against employer justifications, focusing on notice, scope, and proportionality.

In *City of Ontario v. Quon*,[10] the Supreme Court declined to define the outer boundaries of permissible workplace monitoring but clarified the factors that render employer review of electronic communications reasonable.[11] The Court held that a public employer's review of text messages sent on employer-issued pagers did not violate the Fourth Amendment when the search served a legitimate work-related purpose and occurred pursuant to policies placing employees on notice of potential monitoring.[12] Rather than resolving whether employees maintain diminished privacy expectations in employer-provided systems, the Court emphasized that reasonableness turns on the scope of the intrusion and the employer's operational interests.[13] The decision confirmed that employer monitoring—particularly in the public sector—will generally withstand constitutional scrutiny when it remains work-related, limited in scope, and conducted under clear and consistently enforced policies.

The Supreme Court in *O'Connor v. Ortega*[14] articulated the foundational framework for evaluating employee privacy rights in the workplace, holding that public employees may retain reasonable expectations of privacy depending on the "operational realities" of their work

---

[7] *Id.*
[8] 18 U.S.C. § 2510.
[9] *Id.* § 2511.
[10] 560 U.S. 746 (2010).
[11] *Id.*
[12] *Id.* at 764–65.
[13] *Id.* at 760, 764 ("[T]he employer had a legitimate reason for the search, and that the search was not excessively intrusive in light of that justification . . . .").
[14] 480 U.S. 709 (1987).

environment.[15] The Court rejected categorical rules and emphasized that privacy expectations vary based on workplace practices, policies, and the nature of the intrusion.[16] Even where a reasonable expectation of privacy exists, employer searches must serve a legitimate work-related purpose and remain reasonable in scope.[17] Although decided long before the advent of AI monitoring, *O'Connor* provides the analytical foundation for modern surveillance cases, underscoring that technological sophistication does not displace contextual and proportionality-based analysis.[18]

State courts have further refined these principles by recognizing substantive limits on intrusive monitoring. In *Hernandez v. Hillsides, Inc.*,[19] the California Supreme Court held that even surveillance undertaken for legitimate purposes may violate employee privacy when it becomes highly intrusive or disproportionate.[20] Although the court found no liability where a hidden camera inadvertently captured employees in a private office, it emphasized that continuous or covert surveillance raises serious privacy concerns.[21] *Hernandez* is particularly instructive in the context of AI monitoring, where surveillance often operates persistently, passively, and outside employees' immediate awareness.[22] The decision illustrates that legality depends not only on employer intent but also on the intensity, duration, and intrusiveness of the technology employed.[23]

In *Stengart v. Loving Care Agency, Inc.*, the New Jersey Supreme Court adopted a more protective view of employee privacy, holding that an employee retained a reasonable expectation of privacy in personal, attorney-client email communications accessed through a company laptop where employer monitoring policies were ambiguous.[24] The court declined to recognize meaningful consent to surveillance through unclear or broadly worded employee policies or to treat employer ownership of devices as dispositive.[25] *Stengart* underscored judicial concern with overbroad surveillance practices and highlighted the importance of clarity, transparency, and defined limits in monitoring policies.[26] In the age of AI—when employers can collect and

---

[15] *Id.* at 717 (plurality opinion).
[16] *Id.* at 717 ("The operational realities of the workplace, however, may make *some* employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official.").
[17] *Id.* at 725–26 (holding that workplace searches must be "reasonable under all the circumstances" and "not excessively intrusive").
[18] *See id.* at 719–20 (rejecting rigid rules and emphasizing case-by-case assessment).
[19] 211 P.3d 1063 (Cal. 2009)
[20] *Id.* at 1073–74.
[21] *Id.* at 1066.
[22] *Id.* at 1078–79 (recognizing that surveillance may become actionable where it is "highly offensive" in light of its scope, degree, and setting).
[23] *Id.* at 1072–74 (applying a balancing test that weighs intrusion against legitimate business justification).
[24] 990 A.2d 650 (N.J. 2010).
[25] *Id.* at 660–65 (emphasizing the unequal bargaining power between employers and employees and rejecting automatic waiver of privacy).
[26] *Id.* at 665 (criticizing ambiguous monitoring policies and warning against unrestricted employer access to personal communications).

analyze vast amounts of behavioral data beyond employees' reasonable understanding—the case offers a cautionary account of consent and the boundaries of acceptable workplace surveillance.

ETHICAL AND POLICY CONSIDERATIONS

Existing employee privacy doctrine reflects an effort to adapt to technological change, but a growing mismatch between legal frameworks and the realities of AI-driven workplace surveillance.[27] Courts evaluating employee monitoring rely on concepts such as reasonableness, proportionality, and notice to assess the permissibility of employer intrusions.[28] Yet AI systems challenge these principles by enabling continuous, opaque, and inferential surveillance that differs in kind, not merely degree, from traditional monitoring practices.[29] By compiling behavioral, biometric, and location data over time, AI tools can generate predictive insights about employee performance, mental state, or reliability—often without employees' meaningful awareness or ability to consent.[30] As a result, practices that may satisfy formal notice requirements or serve legitimate business interests can undermine autonomy and blur the boundary between work and private life.[31] These dynamics underscore the need to examine AI monitoring not only through existing legal doctrine but also through ethical and policy frameworks capable of addressing scale and power asymmetries in the modern workplace.[32]

AI surveillance raises normative questions concerning the balance of power between employers and employees.[33] It can start even before people are hired: automated hiring algorithms can perpetuate bias and unfairly disadvantage certain groups.[34] Once hired, surveillance can extend to people's homes where they are working remotely or outside of work completely.[35] Should employers be able to use technology to blur—or even collapse completely—the traditional boundaries between work and personal life? This type of continuous monitoring can shape employee behavior, potentially limiting creativity and independent decision-making.[36] It also raises concerns about mental health, trust, and workplace morale.[37]

---

[27] *See City of Ontario v. Quon*, 560 U.S. 746, 759–60 (2010) (declining to articulate broad rules governing emerging workplace technologies); *O'Connor v. Ortega*, 480 U.S. 709, 717–18 (1987).

[28] *See O'Connor*, 480 U.S. at 725–26; *Hernandez v. Hillsides, Inc.*, 211 P.3d 1063, 1072–74 (Cal. 2009).

[29] Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 WASH. L. REV. 555, 560–63 (2020).

[30] *Id.*

[31] *See* Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 321–24 (2010); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1907–12 (2013).

[32] *See Hernandez*, 47 Cal. 4th at 292–93; Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process For Automated Predictions*, 89 WASH. L. REV. 1, 10–11 (2014).

[33] Gabrielle M. Rejouis, *Why Is It OK for Employers to Constantly Surveil Workers?,* SLATE (Sep. 2, 2019, at 07:30 ET), https://slate.com/technology/2019/09/labor-day-worker-surveillance-privacy-rights.html.

[34] Ifeoma Ajunwa, *Unfair Automated Hiring Systems Are Everywhere*, WIRED (May 15, 2023, at 11:33 PT), https://www.wired.com/story/unfair-automated-hiring-systems-are-everywhere-ftc/.

[35] Rejouis*, supra* note 34.

[36] *Id.*

[37] Abril & Harwell, *supra* note 4.

Benjamin Wiseman has suggested that while AI can enhance productivity, it may normalize constant oversight, limiting employee autonomy.[38] In any case, employees should be thoroughly informed about the nature and scope of monitoring, and consent should be meaningful.[39] Even if appropriate boundaries are established and employees meaningfully consent, clear data governance rules must be established. High-tech and AI tools can collect vast quantities of information about workers even within the workplace.[40] Proper handling, storage, and retention of sensitive information are essential to mitigate misuse or accidental disclosure.[41]

CONCLUSION

AI-driven monitoring is reshaping the workplace, intensifying tensions between organizational efficiency and employee privacy.[42] Existing legal frameworks on the federal and state levels are inadequate. They permit expansive surveillance while offering only limited protection against the increasingly omniscient and granular monitoring employers can deploy. Legislatures and courts have also not fully caught up to the need for oversight and employee consent when confronted with powerful tools powered by AI. Meanwhile, employees are losing the autonomy and creativity that are often key to both productivity and worker welfare.

This symposium examines how law, ethics, and policy intersect in the age of AI to identify regulatory gaps, reassess assumptions about consent and proportionality, and propose safeguards that preserve employee autonomy while allowing employers to deploy technological tools responsibly. It will consider policy proposals like limiting off-hours monitoring, independent audits, and strict data minimization protocols that can protect employees.

---

[38] *See* FED. TRADE COMM'N, *supra* note 1; Krouse, *supra* note 2.
[39] Rejouis*, supra* note 34; *see also Artificial Intelligence: Principles to Protect Workers*, AFL-CIO (Oct. 15, 2025), https://aflcio.org/reports/workers-first-ai.
[40] Krouse, *supra* note 2.
[41] Rejouis*, supra* note 34.
[42] FED. TRADE COMM'N, *supra* note 1.