Vol. 3 No. 3 2025
https://doi.org/...
RECOGNIZED IN "Y" CATEGORY BY HEC
Research Consortium Archive
P(ISSN) : 3007-0031
E(ISSN) : 3007-004X
https://rc-archive.com/index.php/Journal/about

Digital Surveillance and the Employment Contract: Corporate Privacy Obligations in the Age of Remote Work

Asma Hanif Sethi
LLB (School of Law), LLM (University of Lahore), DTL (PULC), DCLP (PULC).
asmausmansethi@gmail.com

Publisher : EDUCATION GENIUS SOLUTIONS
Review Type: Double Blind Peer Review

https://doi.org/10.5281/zenodo.16921016

ABSTRACT

The accelerated shift to remote and hybrid work has transformed employee monitoring from an occasional managerial tool into a pervasive, technology-driven feature of modern employment. Powered by "bossware" capable of logging keystrokes, capturing screenshots, activating webcams, tracking GPS locations, and analyzing behavioral or emotional cues, monitoring systems now blur the boundaries between professional oversight and private life. Employers defend these tools as necessary for productivity, compliance, and security—citing insider-threat statistics as high as 60–82% of incidents—while employees and regulators raise concerns about dignity, autonomy, and disproportionate intrusion into personal spaces. This paper situates the debate within statutory data-protection regimes, human-rights jurisprudence, sector-specific compliance frameworks, and the evolving role of the employment contract as the front line instrument for defining surveillance boundaries. Through comparative legal analysis, it identifies the EU/UK model—anchored in necessity, proportionality, transparency, and impact assessments—as the most rights-protective, in contrast to U.S. state-level notice regimes, Canada's emerging provincial disclosure rules, and Australia's state-based statutory guardrails. Case studies, such as Barclays' 2020 "efficiency dashboards" and Microsoft's redesign of its Productivity Score, illustrate reputation, legal, and ethical risks of overreach. The research also examines sector-specific tensions: in finance, strict archival obligations under SEC and MiFID II foster expansive communications monitoring; in the gig economy, algorithmic management and location tracking create asymmetrical power with limited worker recourse, partially countered by "surveillance" strategies. Policy innovations such as "Right to Disconnect" laws in France, Germany, Italy, Slovenia, Canada, Australia, and emerging proposals in South Asia and China demonstrate an international trend toward safeguarding recovery time and curbing off-duty surveillance. The findings highlight that poorly drafted surveillance clauses can extend monitoring into personal time, fail to reflect jurisdictional rights, and undermine trust—while well-designed clauses can embed clarity, proportionality, and respect for worker rights, serving both compliance and cultural goals. The study concludes that effective regulation must combine three pillars: statutory guardrails (necessity, proportionality, transparency), contractual specificity (purpose limitation, scope definition, retention policies, employee rights), and organizational culture that treats surveillance as an exception rather than a default. Recommendations urge multi-level reform: harmonizing legal baselines, enhancing enforcement capacity, mandating data-protection impact assessments for high-intrusion tools, and promoting participatory policy design with worker input. In doing so, employers can meet legitimate operational needs while preserving the fundamental privacy and dignity that underpin a

sustainable and trust-based employment relationship.

Keywords: Employee Surveillance, Remote Work Privacy, Data Protection Laws, Surveillance Regulation, Employment Contract.

Introduction

Remote and hybrid work have made employee monitoring both easier and more tempting, with "bossware" capable of logging keystrokes, taking screenshots, watching webcams, tracking locations, and scoring "productivity" from app usage—a trend that has surged steeply post-2020 as employers cite productivity, cybersquatting, and compliance, while workers seek to preserve privacy, dignity, and autonomy, even when the "workplace" is a bedroom desk. In Europe and the UK, such monitoring is lawful only if it meets GDPR/UK-GDPR standards of lawfulness, fairness, transparency, purpose limitation, data minimization, and proportionality, with "legitimate interests" subject to documented balancing tests and safeguards, and with regulators like the UK's ICO warning in 2023 that intrusive tools, such as always-on webcams or location tracking, require strict necessity and DPIAs, while covert monitoring is exceptional; human-rights jurisprudence, notably *Bărbulescu v. Romania*, reinforces that work communication monitoring engages Article 8 ECHR and demands prior notice and proportional safeguards. In contrast, the U.S. lacks a comprehensive federal privacy law, relying on sectoral statutes, torts, and emerging state-level notice rules such as New York's requirement for written notice and conspicuous posting; Canada's Ontario Bill 88 similarly mandates that employers with 25+ staff document what, how, and why they monitor electronically, while Australia's state-level laws, such as NSW's Workplace Surveillance Act 2005, require advance notice, limit covert surveillance, and control use/disclosure of surveillance records—issues that become more acute when home and workplace overlap. Case studies underscore the reputational and compliance stakes: **Barclays (UK) withdrew** Britain's Information Commissioner's Office (ICO) is investigating Barclays over its use of Sapience Analytics software to monitor employee activity, The Telegraph reported. The bank anonymously tracked staff for 18 months but, in February, reportedly enabled a feature that allowed managers to monitor individuals' time away from desks and task completion times. After staff backlash, Barclays halted the practice later that month and self-reported to the ICO. If found in breach of privacy laws under the EU's GDPR—which the UK still follows—the bank could face fines of up to $1.1 billion, or 4% of global annual revenue, according to Bloomberg, while **Microsoft** altered its Productivity Score to remove individual-level data following criticism as "workplace surveillance," illustrating best practices of narrowing purposes, aggregating data, avoiding constant personal tracking, publishing clear policies, and conducting impact assessments. Even when lawful, intrusive monitoring risks eroding trust, elevating stress, and prompting counter-productive behaviors, with research

from IPPR linking excessive surveillance to morale damage and EU-OSHA highlighting well-being impacts; ethically, the home is not a neutral backdrop, and webcam or audio mandates risk normalizing observation in private spaces. Across jurisdictions, convergence exists on transparency as the minimum baseline, but they diverge on enforceable proportionality: the EU/UK embed it in law and rights jurisprudence; the **U.S.** relies on contractual terms and litigation risk; **Canada's** framework pushes disclosure without proportionality tests; and **Australian** jurisdictions are moving forward with reforms like the "**right to disconnect**," now embedded in federal law through the 2024 amendments to the Fair Work Act allowing employees to ignore work-related communications outside normal hours, except when unreasonable to do so. In Victoria, a parliamentary inquiry recently proposed stronger workplace surveillance laws to limit covert monitoring, require transparency, and restrict the collection of biometric and behavioral data. Under the Australian Workplace Surveillance Act, employers may monitor staff—but only after providing advance notification (typically at least 14 days) or obtaining a court-issued covert surveillance authority when notice is not possible In all cases, the employment contract and related policies are the operational battlefield where legal principles meet practice—defining what signals are collected, for what purposes, for how long, with what rights of access or objection, and what safeguards apply—requiring specificity and accessible explanation rather than buried click-wrap, as regulators increasingly demand clarity, proportionality, and respect for worker autonomy in the evolving landscape of remote-work surveillance.

History Of Worker Surveillance

It is possible that as the market revolution came into play, employers began to experiment on all forms of surveillance in order to work on increasing labor productivity. Curated to focus on the first half of the nineteenth century, market revolution served as a new landmark in the history of industry and it was also one of the first examples of when its bosses were luring more and more Americans to factories to work on their behalf. All that struggling with the machinery in the factories which were then directed by the penned shifts and strict production quotas with a steady beating by the clock was actually much more strictly regulated and defined as compared with the labor that the Americans had once done on farms or in shops which engaged in trade. According to the innumerable historians, this could be described as a time of one of the most profound influences during the history of America.

As the position of the factory labor became rather fossilized, employers became more concerned with precise questions on how they could manage to maximize the productivity by paying extra attention to the activities of the workmen. They combined more often than not work, hour and payment into a conventional formula at the factories. In fact, since most people can easily take Frederick

Winslow Taylor for being one of the earliest management consultants since in 1895 Taylor had published his book, The Principles of Scientific Management, which ultimately provided an outline of an even more intricate order of surveillance and control of a workforce in order to increase the level of productivity. Stories in this period also include the story of Henry Ford that traveled around the factory holding a stopwatch in his hand so as to make his employees more productive and at the same time subjecting the investigators to a personal quest in reviewing the impact of their personal lifestyles on the productivity of his employees.

A fascination among employers to monitor and tweak workers' output has long predates the twenty-first century. Yet one ought to credit the evolution of new technologies for rendering surveillance today far more attainable than it once was. In the end, any firm can only marshal a finite amount of human capital to supervise its operations. In the case of Henry Ford, there are only a finite number of factory-floor managers or private investigators he could hire and assign. Yet new technologies render the surveillance of workers both simpler and less costly. Cameras and sensors can practically be installed anywhere. Smartphones, wearables, laptops, and other internet-enabled tools indispensable for on-the-job tasks can also function at the same time as effective surveillance tools.

Two further developments have further intensified the use of surveillance tools. To begin with, over the past two decades a growing percentage of Americans have taken up teleworking or pursuing their jobs from outside the office. To cite an example, between 2005 and 2012 the percentage of telecommuting American workers surged by 79%. A burgeoning array of online platforms and applications likewise spawned the growth of gig workers. The figure of course soared to unprecedented levels once the COVID-19 pandemic took hold. Amid the pandemic, numerous employers shifted to a predominantly remote-work model. Even though pandemic measures are easing, remote or hybrid setups remain the norm. Since fewer employees now spend their days in physical offices, companies have strengthened their reliance on surveillance tools to reproduce the control they once exercised in the workplace..

Worker Surveillance, Productivity Scoring And Impact On Fundamental Rights

The appeal of new technologies, coupled with vendors' promises of generating actionable "productivity", "risk" or "fit" scores for workers, has led to an array of black-box algorithmic products flooding the market. These tools gather vast troves of data points and run them through subjective rules to assign a worker score or to deduce particular behavioral traits. Such scores can subsequently be employed by human managers to evaluate workers' efficiency, productivity, risk to the company's assets and reputation. Those scores further influence determinations concerning wages, benefits, promotions, disciplinary measures,

and even terminations. In the most extreme cases, the decisions can be fully automated and may no longer need a human manager's review and validation.

When picturing how surveillance and scoring systems function and are interrelated, it may prove useful to divide the process into its component parts. First, an approach to monitor and log workers' activity must be established. Devices—company-issued phones, tablets, wearable fitness trackers and cameras—along with sensors and wireless router networks collect raw data on employees' communications, online activity, movements, and work outputs. Once the data have been gathered, an algorithmic model is required to process the information and draw conclusions or inferences about employees' behavior and performance. Programmers must decide on multiple design considerations—ranging from how data is to be collected to how the resulting AI models will be built. On certain occasions, it may become legitimately necessary to deploy certain data-collection technologies to safeguard workers' safety and security. Another possibility is that legal mandates may oblige the employer to record employee communications. Nevertheless, beyond these narrow warranted cases, the majority of these technologies rest on ill-advised design choices. This paper deliberately uses the term 'surveillance' instead of 'monitoring.' The notion of surveillance recognizes the authority employers wield over workers and the omnipresent capturing of worker communication, engagement, and interaction data, most of which is deployed solely for the employer's own benefit. Consequently, such data would permit employers to exert control and influence over workers' engagement and, where applicable, guide the provisions of their contracts.

According to providers of these scoring systems, the surveillance data gathered is purportedly ripe for inference about workers' productivity, risk status and suitability for their particular roles. Claims and embedded design choices rest on inherently false premises, such as technology's power to faithfully capture a human's intricate nature, to discern emotions and sentiments, or to reliably predict human behavior. These surveillance and scoring technologies likewise impinge upon an individual's rights and freedoms. These technologies, together with the assumptions embedded in them, may conflict directly with fundamental human rights. Even though these technologies cannot fulfill their marketing assurances, they continue to attract purchasing decisions from business decision-makers.

Human dignity: Even when workers understand the intrusive surveillance at work, they often lack the opportunity or the means to resign because they worry about the intrusive data collection and the arbitrary action of algorithms. Should further consent be requested at any point at all, workers are asked to trade their data for the prospect of earning a wage. They will invariably opt to preserve their employment. Under these power imbalances, a

worker's consent cannot be considered either free or informed. The workers forfeit control over their personal privacy—over the employment of their bodies, their movements, and even their social interactions. Who is best situated to set the parameters delineating the information indispensable to an employer? Lacking either legal safeguards or concerted labor action, the workers are left to contend with surveillance on their own. The boundary is marked 'on' their bodies.

Human dignity is again eroded within these scoring models, as human complexity, engagements, aspirations, and creativity are crunched into numerical figures and tenuous correlations. No human narrative under-girds the interaction, and employees can no longer 'bring their whole selves to work.' Employers and vendors pare the worker down to a set of metrics they deem significant and that can be efficiently gathered.

Ifeoma Ajunwa further notes that wearable data-tracking tools can give rise to fresh legal questions, among them the risk that an employer could violate the National Labor Relations Act standard for unlawful surveillance—observing workers in concerted activity "in an atypical manner that is therefore coercive." These tactics likewise erode key principles embraced in the Fair Information Practices—including collection limitation, purpose specification, use limitation, accountability, security, notice, choice, and data minimization. Case in point: topical examples include third-party data—such as wellness or insurance-provider–sponsored fitness devices—collected through an employer and later repurposed to limit a worker's access to resources and opportunities outside the organization.

Right to privacy: Breaches of privacy constitute one of the foremost points highlighted in discussions of worker surveillance. It is generally viewed that the right to privacy constitutes a fundamental human right. Within the United Kingdom, Barclays Bank could incur a $1.1 billion fine for its alleged monitoring of employees. In Germany, the data protection authority iss Nevertheless, in the United States, employers are allowed to gather data whenever employees access the organization's devices or network infrastructure. Devoid of federal privacy regulations, an independent data-protection watchdog body, and any statutory limits on worker surveillance, current conditions permit employers to act as they please in furtherance of their own interests. Yet legal does not inherently imply ethical.

A recent OECD working paper on AI in the workplace observes that the adoption of AI systems can magnify and structure ethical shortcomings while fundamentally altering the dynamics between workers and their managers. Certain surveillance techniques intrude on the boundary between work life and personal life, empowering employers to collect highly personal information about their employees. For instance, employers might conduct (1) social-media monitoring, (2)video surveillance on premises,

(3)require employees to keep their laptop cameras on—or compel them to employ smart assistants that record conversations—or (4)capture employees' computer screenshots at random intervals. During 2022, a Dutch court held that an employer compelling workers to leave their webcams active for prolonged periods each day and share screens on their devices breached the workers' right to respect for private and family life. In Germany, the data protection watchdog levied a $41 million penalty against retail giant H&M for conducting illegal employee surveillance and compiling "excessive" dossiers containing details on its workforce's families, religious beliefs and health conditions. Likewise, the European Court of Human Rights handed down a comparable decision in 2017. This level of monitoring may likewise expose information shielded by Title VII of the Civil Rights Act of 1964—such as sex, race, color, national origin or religion, sexual orientation, etc.—or the Americans with Disabilities Act ("ADA").

Despite the prohibition on using protected information in employment decisions, employers' knowledge of such details can still trigger possible subconscious biases. Surveillance focuses on the employee instead of their activities on the job. Exposure to this protected information that the employer would not otherwise have been aware of can generate legal risks for the employer and invites potential claims of discrimination..

Right to Expression: The capacity to monitor workers' private and social exchanges erodes the freedom of expression. Through the surveillance of emails, chats, and phone calls, employers can eavesdrop on employees' thoughts without differentiating between what is personal and what is professional. Awareness of being survived may compel workers to censor their own expressions and ideas. Manokha's restatement of Foucault's 'technologies of the self' stresses how surveillance plays into individuals' self-restraint and self-discipline. Under such conditions, employees might impose self-restraint while fully conscious of being watched, thereby making no response to corporate coercion or physical force. Employers' quest to monitor workplace communication likewise intrudes into areas of employees' personal lives. An increasing number of firms now monitor workers' and prospective employees' social media profiles, and some have even patented audio surveillance tools capable of overhearing communications between employees and customers. Certain firms insist on access to employees' social media accounts in order to monitor them. In those states that legally safeguard this boundary, employers can still persist in the practice by partnering with third-party vendors. Such vendors analyze both candidates' and employees' social media footprints and, as needed, furnish employers with either one-time or sustained risk ratings. Although risk scoring models can produce spurious correlations, many employers nevertheless rely on those results as a third-party metric for their hiring decisions. The prospect that employers will scrutinize and even

react to their social media content may discourage employees from fully expressing their genuine identities (i.e. sexual orientation, faith, physical or mental ability, etc.) beyond the workplace. Workers may likewise decide not to post on social, economic, political, or other societal issues. Such trends may ultimately give rise to substantial societal repercussions.

Right To Data Protection: Data gathered through AI surveillance technologies is occurring universally and with great breadth. Devoid of federal privacy legislation and comprehensive worker safeguards, employers can not only amass data but also pass that information onward to third parties for a variety of purposes. Employees have no ability to review the data amassed about them and likewise cannot influence how the data-collecting entity might use that information. In most cases, workers have little comprehension of the intricate nature of the data, the conclusions drawn about them, or the potential scope of any consequences. Studies by the UC Berkeley Center for Labor Research and Education and CoWorker.org alike find that the collection of such data is not governed by clear and uniform safeguards. Any breach of the data may affect the worker's access to benefits, resources and opportunities beyond the workplace.

Collective Action And Power: Surveillance assembles a group that makes the decision to monitor and collect information, and reaps the benefits derived from the resulting data; it also compels another group, which bears the impact of that decision. If workers seek to challenge this imbalance by engaging in individual defiance or coordinated action, such data may itself function to stifle lawful collective activity such as unionization or grievance. Put another way, employees without ample safeguards are unable to mount a strong resistance to intrusive surveillance, and in some instances the very system is exploited to dissuade and block unionization efforts.

History is replete with instances in which corporations enlist private investigators to monitor workers' activities so as to suppress collective action and break strikes . Released in 1987 by the United States Office of Technology Assessment, the study "The Electronic Supervisor: New Technology, New Tensions" offers a historical survey of the tensions and accompanying concerns triggered by electronic employer surveillance systems. Privacy, fairness, and the standard of work life are identified as the key concerns in the report. Within the fairness discussion, the report cites "reasonable standards, knowledge by employees of how the monitoring system functions and the limits thereof, whether employees can dispute or amend recorded data, and their involvement in helping develop the system." The report notes that U.S. statutory law imposes no obligations for employers to ensure monitoring is "fair," tasks are well-designed, or employees are re-consulted on work standards, save where such matters are covered in union contracts.

Alas, three and a half decades after its release, unionization levels have fallen below what they were in 1987, technology permits more intrusive data gathering, and unions' internal capacities to resist these surveillance measures remain seriously lacking. As the capacity to gather omnipresent data grows, employers can leverage emerging technologies to wield power over their workforce. With this informational gap, algorithms intensify the firms' grip on power while affording workers no counterweight. Spain introduced a law in 2021 obliging online delivery platforms to notify unions whenever algorithms mediate workers' working conditions.

Employers are likewise compelled to submit "Surveillance Reports" that disclose certain expenditures and arrangements pertaining to labor disputes. It is plain that the expenses encompass expenditures on surveillance technologies and activities. Yet, because workers and labour unions seldom know of covert surveillance, it becomes difficult to hold employers to their transparency commitments or contend against unfair practices. According to scholars Pasquale and Citron, "keeping unfair practices under wraps is a discriminator's most potent ally: unseen injustices cannot be challenged, let alone rectified." Recognizing data rights for workers through collective agreements thereby safeguards workers while guarding against any erosion of union strength.

Workers' right to engage in gainful employment, along with the right to remuneration commensurate with fair and decent working conditions:

Emerging AI technologies are progressively enabling previously disparate datasets to be linked. ProPublica's excellent investigative piece explains how this software sold to landowners equips them with data about local occupancy rates, rental figures in their area, and the option to communicate with one another through the platform. Where earlier landlords were compelled to expend considerable resources to compile this information separately, today's platforms and technological services provide users with real-time, up-to-date data. Possession of this data can be leveraged to intensify market pressures and adjust vacancies so that rents climb above their market equilibrium. One may likewise draw a parallel between how wage levels and labor rights intersect in this scenario. In addition, tools such as Argyle furnish aggregated workforce financial data to employers via applicant tracking systems and send that information to insurance providers, lenders, and credit card issuers via a unified API. Argyle seeks not only to supply financial data, but also to offer a holistic view of a worker's identity—spanning typical hours, work trajectory, reputation, and other characteristics. Put differently, it supplies employers with a unified view of a candidate's employment record and other compensation-related data before an offer is extended. Due to this imbalanced flow of data, employers can pay insufficient wages or join forces with other companies to suppress wage levels.

Argyle states that it currently profiles more than 175 million workers, representing roughly 80% of the U.S. workforce. Though the vendor bills itself as a "third-party verification platform that permits workers to safely transmit their income, job title, and proof-of-employment data to lenders, background check agencies, human resources, and other recipients of their choice," the vendor offers no explanation about the magnitude of data it collects, how it may be subsequently employed, or the attendant risks to workers. Furthermore, many workers could forfeit the possibility of future prospects because the filtering software widely adopted by employers in the industry consigns their profiles to perpetual inaccessibility.

If algorithmic systems begin feeding one another inputs, or if employers start relying more often on aggregated systems to shape pre-employment decisions, an additional risk arises. An outcome biased, inaccurate, or deliberately manipulated by one system feeds directly into the next decision-making system. As these interconnected systems entwine, workers can be permanently barred from accessing affordable housing, insurance, health care, and parallel programs.

In matters of validity and opaque decision-making: vendors crafting the scoring algorithms frequently boast about their products' abilities without disclosing the formulas used or the design choices embedded within the system. Should a client insist on seeing the science that underpins the system, it may collapse like a house of cards. Rather, the vendor is inclined to hide behind intellectual property (IP) safeguards and urge the employer to trust the purported neutrality of the technology. Nevertheless, skimping on rigorous vetting can leave employer clients liable. A client has every right and mandate for transparency. Unfortunately, since vendors and employers each derive separate advantages from these technologies, ensuring their scientific soundness—or even questioning whether they ought to exist at all—has been made a low priority.

Even after an employer recognizes that the technology fails to meet its promised outcomes, it might nevertheless keep the practice in place, simply because it provides a means of gathering information about workers' activity. The employer could elect to remedy the shortcoming by adopting an additional tier of surveillance. As illustration, when an AI-driven system designed to monitor workers' movements in an Amazon warehouse malfunctions, the footage is routed to workers in India and Costa Rica. Those employees supply feedback that helps refine Amazon's surveillance machine learning algorithms. The workers "don't know where the specifics of that data are heading, nor what goes on behind the scenes." Moreover, those employees working remotely were surprised to learn that their screen and mouse movements were likewise being tracked and monitored.

Civil-process right: Data-centric technologies "mask, erase, and

affirm employer conduct beneath an opaque algorithm ." Scores can trigger automatic deductions to wages, shift allocations, and on occasion even outright termination. Because they lack insight into how the surveillance and productivity-rating algorithms shape their pay, benefits, or working conditions—or into the safeguards that unions embed in their contracts—"workers are left with no effective means to contest harmful employer actions like discrimination and wage theft." Across many jurisdictions, employees further contend with algorithms shielded by intellectual property law. Consequently, even if employees or unions have the capability to scrutinize algorithmic models, they might not be able to lay eyes on them. Individuals whose labor and productivity are analyzed and calculated through these algorithms merit stronger protections, notably a right to procedural data due process. Across the United States, the majority of workers in low-wage positions labor under an "at will" framework that permits both employer and employee to terminate the relationship free of any justification. Nevertheless, a variety of other employment decisions could still benefit from being subject to due-process requirements.

Normative determinations: When creating the scoring models, developers reach specific decisions. Among these choices are which activity's data should be captured—in other words, which behavior or action counts toward productivity or risk. Developers decide which data set can technically be captured and which of those metrics will function as a proxy for productivity. They set normative standards for what constitutes 'normal' or 'typical' productivity and, subsequently, evaluate workers' data against those benchmarks. They pin down the labels and place workers into their respective categories. By reducing people to predefined classifications, developers likewise dehumanize and depersonalize the employees. In the course of making these choices, developers likewise pen their own values, experiences, cultural frameworks and biases into the algorithms they create. In a recent New York Times piece on worker productivity monitoring, the problem is conveyed as "the modern workplace's timekeeping devices are fundamentally misaligned: they miss offline activity, falter at appraising hard-to-measure tasks and often end up compromising the work itself." Should developers choose to prioritize certain factors—or should they neglect to account for all pertinent ones—the outcome can be unintended consequences.."

By enforcing one unified benchmark for all, these algorithmic systems compel uniform behavior, propagating uniformity. Charlie Munger, Berkshire Hathaway's vice chairman and one of the most successful business investors, observes that copying the herd tends to produce only average results—a "regression to the mean." As companies across the globe seek to woo prospective candidates from varied backgrounds, experiences, identities and perspectives, they devote considerable time and resources in the effort. By relying on surveillance and rating mechanisms to assess workers'

adherence to specified norms and behaviors and to stifle diversity, employers undermine their own long-standing objectives.

In much the same way that algorithm designers immature normative judgments into their scoring systems, they likewise insist upon their products' universal applicability. Yet anyone who has journeyed across different regions of a nation or overseas can vouch that cultural disparities mirror themselves in working relationships. Across cultures, prevailing workplace norms differ and the ways employees interact with one another are likewise varied.

Even in a setting of uniform corporate culture, scoring systems still fail to grasp the intricacies of work and overlook the external factors that may hinder a worker's capacity to produce an output or finish a task within a preset time frame. By overlooking the context of workers' interactions and the full effort expended in producing an output, such systems elevate quantity and quantification to the implicit priories, overshadowing quality and the depth of the work. Data stands in no way independent from its surrounding context. Workers living with productivity algorithms often refer to the set-up as "infuriating", "soul crushing" and an all-out "kick in the teeth," pointing out that employers failed to recognize the full complexity of all the tasks involved in their role. Employers demand that their employees act like robotic subjects. Thereby, this strategy provides no space for diverse perspectives and no recognition of offline tasks, such as thinking, reading print materials, collaborating with colleagues during brainstorming sessions, or mentoring fellow employees.

Disability discrimination: Such systems that assess productivity by projecting an "average" expectation may rise to other harms for people with disabilities. Several Analyses of the ADA imply that a firm that imposes a demanding pace-of-work benchmark and applies it inflexibly may violate the statute's ban on "standards, criteria, or methods of administration ... that discriminate on the basis of disability." Because more than half of disabilities are unseen and their conditions are highly diverse, they are virtually impossible to analyze at scale. Moreover, just over a fifth of employees with disabilities disclose that information to their employers' human resources departments. The use of biometric or health data gathered through wearable or other sources linked to workers' social media profiles can feed managers or employers with extra information to presume about an employee's abilities or condition, which, in turn, may yield inequitable choices or inaccurate conclusions. Even when the information does not factor into a negative hiring decision, an employer may nevertheless be accused of discriminating on account of a disability or perceived disability.

Deficiencies in the AI's architecture, ranging from device-level imprecision to bigger structural flaws, may likewise lead to unforeseen harms. For instance, wearables gathering health and

wellness metrics might not be precise to start with; nevertheless, they can still be leveraged for employment-related assessments. Because the system's scientific validity—and any inherent technical biases—remain unscrutinized, workers are liable to face discriminatory outcomes. Imagine further that the system's developers—or its employers—remain oblivious to any bias embedded inside it. For instance, assistive technologies (e.g. screen readers) can compromise the precision of the data that are recorded. If such assessment tools disadvantage neurodivergent students, readers who progress more slowly, or multitaskers, the ensuing outcomes may amount to discrimination.

Eroding trust: The history of worker surveillance abundantly illustrates how employers opt for the simpler course of monitoring workers instead of investing in building trust and a mutual vision with them. Frequently, organization opt for textbook hierarchies, favoured for their ease of control. By contrast, the option lies in collaborative co-creation of joint values and vision. Steering value creation and holding themselves and their employers accountable to the agreed outcomes, the workers were entrusted with this responsibility. In the absence of mutual trust, employers corrode workers' own trust and loyalty. As the COVID-19 pandemic pushed adoption of work-from-home roles, numerous employers were plunged into a state of panic. According to an article in the Harvard Business Review, "A vicious cycle emerges when managerial distrust breeds micromanagement, which in turn saps employee motivation and consequently hampers productivity." And thanks to the COVID-19 pandemic, this spiral descended to even greater depths. A recent Microsoft study shows that 85% of leaders now report that the transition to hybrid work makes it difficult for them to feel confident about employee productivity. Be it supervising remote employees, those in large workplaces such as warehouses and shops, or mobile workers (e.g., drivers and delivery personnel), or those who have resorted to "quiet quitting," the adoption of surveillance and productivity tools fractures the trust bond beyond repair and can ultimately undermine productivity.

Effect on Health and Safety: Greater pressure on accelerated pace-of-work and heightened productivity targets, coupled with no time for rest, thinking or rectification, result in increased workplace accidents. Within the "electronic sweatshop," employees are tasked with monotonous, rapid-tempo activities that imposed unceasing vigilance and meticulous attention to detail. Greater repetition likewise gives rise to more severe physical injuries. Scholarly studies reveal that workplace performance-tracking technologies are linked to heightened workplace stress. A reduction in individual control over tasks, mounting stress, and omnipresent surveillance heightens the likelihood of psychological distress and worsened mental well-being for workers.

At times, employers portray productivity scoring systems as nothing more than games. In summary, by disguising labour as a

string of competitive indicators, employers set their workforce in competition with one another. By rendering the productivity metrics public, employers may add an extra layer of stress to the workforce. Even when this competition is rolled into a wellness program, normative assessments of workers' fitness and health are still impressed upon them. For instance, obligating staff to hit prescribed fitness benchmarks—and exposing for all co-workers the data of anyone who falls short of those expectations—can be regarded as a form of body-shaming. Striving to fulfil the expected metrics, coupled with rising stress and wear on physical health, ultimately culminates in workforce burnout. When a corporate culture treats a worker's role as interchangeable with that of the person who will take their place, and when no legal repercussions apply, employers have no compelling reason to improve working conditions.

Feedback loops and behavioral shift: Algorithmic decision-making systems alter the actions of their users as well as of the individuals affected by their outputs. In many ways, they modify and mold the organization's culture and priorities. By rewarding employees for concentrating on one task rather than on innovation and experimentation, the organization implicitly communicates to its workers through the decisions about what it monitors. In productivity systems, employees may end up devoting more effort to an activity that is logged and rewarded than to actually producing results. The metric thereby stands as its own objective. Surveillance functions to train workers toward conformance to behavior that can be quantified. If workers' independence and agency are curtailed, the impact includes a narrowed ability to be inventive and to "think—and sometimes act—outside the box."

Should workers come under surveillance and fear that their scores will determine their pay or future prospects, they will therefore naturally start adopting more self-protective postures. Rather than cooperating with fellow employees or divulging insights into more efficient approaches to finishing tasks, individual workers may grow more secretive, suspicious and desperate to out-compete one another. They might likewise become compelled to game the system. Be it a response to employers' oppressive measures, or driven by the wish to up their scores (and thereby their wages and benefits), gaming the system entails devising ways to appear as though one is working diligently, while secretly shirking the tasks required. In the face of management's lack of trust, employees might look for ways to sidestep intrusive managerial control [87].

The constant vigilance surrounding pervasive surveillance and datafication likewise undermines workers' morale and diverts attention from other tasks that might be both meaningful and vital to long-term well-being. Dependence on the evaluation of only select tasks may oblige employees to reach decisions swiftly, often without the time to explore an issue, case or condition in depth. In

this regard, some scholars further contend that gamified workplace environments may entangle and undermine ethical judgement. In professions where rapid, ongoing decisions are routine—such as health, human, and social services—such a behavioral shift may have catastrophic consequences for those who rely on those decisions.

Legal Frameworks & Boundaries

In the U.S., employers typically enjoy broad leeway to monitor employee activity on employer-provided devices and networks. Courts generally uphold such monitoring, especially when aimed at cybersecurity or productivity, so long as personal communications are not unlawfully intercepted. For example, edicts under the **Electronic Communications Privacy Act (ECPA) of 1986** prohibit unauthorized access to electronic communications—but carve carve-outs for employer monitoring when consent is given or the monitoring falls within the "ordinary course of business."

Pragmatically, organizations often rely on two main ECPA exceptions: **(1) consent**, by way of signed policies acknowledging monitoring, and **(2) ordinary-course-of-business** needs, like preventing data leaks or ensuring system integrity. But this creates a "**tightrope walk**." Without clear policies, employers risk statutory (federal) penalties—up to $250,000 in fines, prison terms, or civil suits—and reputational damage.

In the **European Union**, employee monitoring is permissible under the GDPR (Regulation 2016/679)—the global benchmark for data protection—but must adhere to strict principles such as lawfulness, transparency, necessity, purpose limitation, and data minimization. The EU Charter of Fundamental Rights (Article 7) and the **ECHR Article 8** further protect privacy at work, underscored by landmark judgments like Bărbulescu v. Romania, where the European Court held that employees retain a "reasonable expectation of privacy" and employers must provide notice before monitoring personal communications. Moreover, **Directive 2002/14/EC** mandates that employee representatives be informed and consulted when significant changes—such as the introduction of monitoring technologies affect workplace practices
In the **UK, EU**-aligned rules continue under the **Data Protection Act 2018 (supplementing the UK GDPR) and the Human Rights Act 1998**, which embeds ECHR protections into domestic law. Workplace surveillance—like intercepting private emails or audio requires "lawful authority," and employees must be able to maintain a baseline level of privacy even on company systems The ICO's guidance closely mirrors GDPR principles and emphasizes transparency and proportionality, particularly in remote-monitoring contexts

Beyond Europe, some **Australian** jurisdictions are moving forward with reforms like the "right to disconnect," now embedded in federal law through the 2024 amendments to the Fair Work Act allowing employees to ignore work-related communications outside

normal hours, except when unreasonable to do so. In **Victoria**, a parliamentary inquiry recently proposed stronger workplace surveillance laws to limit covert monitoring, require transparency, and restrict the collection of biometric and behavioral data. Under the Australian Workplace Surveillance Act, employers may monitor staff—but only after providing advance notification (typically at least 14 days) or obtaining a court-issued covert surveillance authority when notice is not possible.

In **Canada**, privacy protection is grounded in the federal PIPEDA, governing private-sector personal data use, alongside provincial laws like those in Quebec and British Columbia. Employers must follow principles of notification and consent, though rules vary by jurisdiction and context. Ontario courts have also recognized a common-law tort of "intrusion upon seclusion," further bolstering employee privacy rights. In **Pakistan**, workplace monitoring remains largely unregulated beyond the general cyber-crime framework of PECA, although a 2023 draft Personal Data Protection Bill proposes establishing a National Commission for Personal Data Protection and limiting sensitive data processing yet no clear transparency or proportionality rules currently bind employers (PECA entitles imprisonment and fines up to PKR 5 million for unauthorized data use) . In **India**, while there's no express workplace-monitoring law, the Information Technology Act and SPDI Rules require consent for collecting sensitive employee data, and the landmark privacy ruling (Puttaswamy) affirms a constitutional right to privacy. The Digital Personal Data Protection Act, 2023 (DPDP Act)—enacted on August 11, 2023—introduces broader principles like purpose limitation, data minimization, accountability, employee notice, grievance redressal, and permissible "legitimate uses" for employment-related processing, though it has yet to be fully enforced and rules are still pending

Surveillance Practices & Employer Justifications

The current wave of employee surveillance technology (sometimes called bossware) includes a package of capabilities far beyond what could have been done through the traditional methods of the past; scholarly, legislative, and journalistic examination is increasingly revealing what is possible, and why this is a concern. Keystroke logging and mouse tracking is perhaps the most ubiquitous form of surveillance and would capture typing speed, rates of error, programs which are being used and even cursor movements around the screen. Because such systems can build in-depth behavioral profiles, as Wired and scholarly research at UNSW point out, this is not only possible to evaluate individual performance but it is also possible that behavioral patterns are detected that an employer can interpret as lack of engagement, or failure to comply.

This is complemented by screenshot capture at specific intervals or even randomly, return a literal view to the managers of the workers desktop actions. According to the European commission Joint Research Centre such practices particularly when

accompanied by metadata such as time stamps and file names may have a line moving between verification of tasks and intrusive monitoring of personal interests or casual personal data.

More controversial is the introduction of webcam and microphone activations during remote sessions, which has the capacity of recording photos or background noise on the employee home setting. This is electronically legitimized by some companies to confirm attendance or through participation in meeting, but poses a major potential breach of data privacy law (GDPR) and human rights law in Europe, and analogous privacy conflict in different jurisdictions, with references to domestic living quarters and household members involved.

Location tracking using GPS-enabled technologies, corporate cell phones, or even the swipe of physical badges makes the physical area a part of surveillance where the movement of the workers is being tracked either on-site or off-site. PMC peer-reviewed resources, as well as various legal discussions, highlight the ability of this tracking when not necessarily limited by purpose and need to detect sensitive location data not related to work (medical treatment, political action).

These modes share one commonality in the credible literature: that although the narrative purpose is productivity, security, or compliance, the practical result is that managerial authority insinuates into the most personal aspects of employee lives, particularly in hybrid and remote work environments, thereby necessitating transparency, proportionate governance, and, where possible, necessity as not only an ethical requirement but a legal requirement, as well (in most locations).

Employer Justifications: Productivity, Security, and "Control"

Employee surveillance is often framed by employers as a mechanism to **boost productivity, ensure accountability, and manage operational risks**, yet empirical evidence and ethical analyses reveal a far more complex picture. Historically, monitoring of email and internet use was already widespread by 2007, with documented disciplinary actions—including terminations—underscoring its punitive edge. Today, more sophisticated tools deliver **real-time activity tracking, attendance logging, and performance scoring** (Wired), but their impacts are mixed. Employers also justify surveillance for **security and insider threat prevention**, citing data that insider actions account for 60% of incidents (IBM) and up to 82% (Verizon), particularly in sectors handling sensitive or regulated data. In compliance-heavy industries, monitoring serves to meet legal obligations—such as safeguarding financial records or documenting workplace communications—while also defending against harassment claims or other legal disputes (Skadden, Touro Law). Yet beyond these practical justifications lies what some scholars term the **illusion of control**: digital dashboards, behavioral alerts, and attendance metrics centralize managerial power, often without delivering

measurable productivity gains (Equitable Growth, SSRN).

Empirical Consequences and Ethical Backlash

Empirical studies challenge the productivity narrative, showing that **excessive monitoring can backfire**. Arizona State University research found that heavily monitored employees tend to work slower or take unscheduled breaks, and 43% engage in "productivity theater"—performing unnecessary actions to appear busy (Toggl). Furthermore, 75% report reduced job satisfaction under surveillance. Psychological research, including the EU Joint Research Centre's analysis, links intrusive monitoring to **stress, diminished well-being, and higher turnover**, with UK media noting disproportionate harm to vulnerable groups, especially where tools include emotional analytics. From a techno-ethical perspective, surveillance erodes worker dignity and autonomy, undermining even utilitarian defenses since the harms—stress, mistrust, reduced morale—often outweigh claimed benefits (arXiv, PMC). Workers increasingly respond with **resistance tactics**, from automated "mouse jigglers" to fake activity logs, signaling both distrust in management and inadequacy in current policy safeguards (Wired). Collectively, these findings indicate that while surveillance can fulfill legitimate aims, without strict **necessity, proportionality, and transparency**, it risks becoming a counterproductive tool of control that damages the very performance and culture it seeks to protect.

Case Studies:

Time Doctor Webcam Absurdity A Reddit exposé described forced webcam snaps every 7–10 minutes by company "Time Doctor," even flagging employees for looking away or stepping off-screen—leading to humiliation and required defense for small infractions. **AI Emotional Analytics in Call Centers** In the U.S. and Canada, corporations using emotion-tracking tools have fired workers based on inferred mood metrics. One customer-service worker shared being terminated after her monitoring system judged her tone to be too negative. **Amazon Warehouse "Panopticon"** At Amazon's warehouses, every step of a worker's day is monitored by a web of sensors, cameras, and AI. From the moment Rina swipes her ID badge and passes through security, her location is tracked, her pace measured, and even her choice of break room can affect her tightly controlled 30-minute lunch. At her station, she must inspect 1,800 items an hour under constant scanning, while any pause—whether for the bathroom or a slowdown in conveyor traffic—is logged as "time off task," potentially triggering discipline or termination. When her shift ends, she undergoes anti-theft checks before leaving. This is surveillance as a management system—where technology doesn't just oversee work, but actively shapes how, when, and even where a worker moves, blurring the line between efficiency tracking and total behavioral control.

Big Brother, meet "bossware" LaIn February 2005, after 18 years of employment, Insurance Australia Group terminated st year by

February because she was unable to sustain the number of keyboard hits that she was given on a computer. After the analysis of broader spectrums of performance standards, the Fair Work Commission overlooked her against unfair dismissal complaint. A Canadian lady was told to repay 4142 dollars to her former employer because a monitoring program in her laptop made her believe that she has fraudulently billed 50 hours of work. It was because of time theft that she was fired by her employer. She did not only work on the laptop according to her. In spite of this, a tribunal found that the tracking software furnished sufficient information towards misconduct. The phenomenon of surveillance in the labor force has already far surpassed large tech enterprises and is typified by the number of smaller firms that market their products as a service to track every aspect of work process particularly in the circumstances of undermining the rights of employees as applied. This greater surveillance is one which extracts more out of the employees and provides less in exchange and in such a way it establishes a culture of discrimination which kills off privacy and further frustrates the right to organize and even the division of home and work. These systems gig-ify labour by splitting it up into measurable activities that isolate individuals and direct their activities through constant monitoring as set in the old laws loopholes which in turn have always alienated the weak communities and the other is by evading employer obligations, like providing good wages or benefits. The surveillance does not just oversee the productivity, but also, regulates the organizing, tracks the workers online where they engage in communication, and uses communication tools turning them against the workers by utilizing them as a union-busting gadget. The point is that modern monitoring of employees is not a strategy of profit maximization only, but it is also a demonstration of the force as guidance over the actions, time, and relative of the employees, and it outsmarts the rules with the corporate influence which may take the activities beyond the range that the rules would respond.

The Roadmap

There are several policy solutions that could be introduced to ensure better protection of the employees against the proliferation of digital surveillance and productivity-ranking network. Going back to the already existing U.S. policy and regulatory provisions, we can find our way ahead.

Bring the same safeguards embodied in the Privacy Act of 1974 into force within labor regulations.

The CFLP and its companion, the FLSA—both enacted to set forth minimum wage, overtime pay, record-keeping, and child labor benchmarks for workers in both the private and public sectors—either directly or indirectly informed the development of FIPs. The FIPs outline the rights and duties regulating the collection and processing of personal data, placing equal emphasis on practical standards and on formal legal rights. Upon passage of the Privacy

Act of 1974, Congress enshrined eight principles to regulate the information on individuals held in federal agencies' databases. Tracing the initiative back to its roots, labor regulations ought to be revised. The safeguards afforded under the 1974 Privacy Act ought to be broadened to cover existing labor legislation. The responsibilities of employers and the rights of workers must be expressed with definite clarity.

- Collection limitation/Data minimization: employers are allowed to create, collect, use, process, store, maintain, disseminate, or disclose data only when that information is directly relevant and necessary to achieve a legally authorized purpose.
- Quality of the Data: collected information must be pertinent to the purposes that employers intend to employ it. Employers are obliged to verify that the data in their possession is accurate, relevant, timely, and complete.
- Purpose specification: employers should disclose their planned use of the data prior to collecting any information.
- Utilization limitation: once employers has collected data for a stated purpose, they may not subsequently use that data for any other purpose.
- Security safeguards: employers must make certain that any data they collect are securely stored.
- Individual participation: workers must be granted the rights to obtain, verify or confirm any personal data collected about them, to obtain a copy of that data promptly, and to have the data they provide erased, rectified, completed or amended should they prefer so.
- Openness: employers must remain transparent in the procedures through which they formulate data-collection policies.
- Accountability: employers are required to establish a mechanism for keeping track of their adherence to the principles listed above.

It should be noted that Article 5 of the EU's General Data Protection Regulation (GDPR) catalogue all FIPs except Individual Participation, a category that is designated in its own sections in other GDPR articles.

During the 1991 rollout of S. 516—the Privacy for Consumers and Workers Act—Marc Rotenberg and Gary Marx each delivered individual testimonies before the legislators. Even though the legislation did not advance at the time, it is still notable the contributions they each offered that could fortify any future labor legislation.

Marx exposed the techno-fallacies embedded in worker surveillance practices and set out:

- Validity principle: adequate grounds must exist for assuming the accuracy and value of the information collected.
- Redress principle: individuals whose privacy is compromised

must be supplied with adequate means by which to detect such violations and secure compensation.
- Safety-net principle or equity principle: an essential baseline of privacy is promised to every individual..

Rotenberg vigorously backed the draft legislation, demanded the backdoor exclusions be stripped out, and proposed additional safeguards in the form of:

- Worker participation: Workers should take a central role in defining the technology that affects them. Any employer intending to collect data ought to pursue wider forms of co-determination and to involve workers openly, joining them with the employer in defining the conditions governing the use of that data. Beyond the worker's individual participation, that body of employees could also exercise a collective right to take meaningful part in—and co-determine—the processes governing every aspect of their assessment. Such co-determination might evaluate the potential effects of an algorithmic system, gauge its suitability as a valid solution, and, where appropriate, make choices about the pertinent data, the system's algorithmic design, and the overall governance of its operation.
- **Business responsibility:** Employee information that is collected is protected.
- Human review principle: technology should empower, not supplant, human judgment in making key employment decisions.

Putting into practice the Blueprint for an AI bill of rights.

Nowhere is this more starkly articulated than in the recently released Blueprint, in which the design of employee-facing surveillance systems is urged to place employees' rights at the forefront of considerations. These guidelines articulate a future course for AI's development and use that honours human rights, democratic values, and fundamental principles. The vision therefore requires implementation. In particular, the Blueprint urges

- That such technologies "be subject to rigorous oversight, at a minimum beginning with a pre-deployment evaluation of their potential harms and with firm limits on their scope to safeguard privacy and civil liberties."
- Continuous surveillance and monitoring should therefore be prohibited in... work...where the deployment of these surveillance technologies is anticipated to curtail rights, opportunities, or access.

The Blueprint recaps the fundamental rights, existing civil-rights statutes, and anti-discrimination laws. The Blueprint's foundational vision ought to serve as an instrument for strengthening existing employment laws, labor-relations statutes, and workplace safety measures. The Department of Labor, as well as the pertinent federal agencies—such as the Equal Employment Opportunity Commission,

National Labor Relations Board, and Occupational Safety and Health Administration—should integrate the Blueprint's implementation into their current strategic plans. Although the current statutory architecture and precedent can correct harm, EEOC can also draw on complementary tools—such as the Commissioner's Charge or a directed investigation—to uncover potential systemic discrimination. As previously discussed, workplace surveillance has become far more prevalent than it once was, making it imperative and vital that these agencies view this issue as properly within their area of responsibility.

Enforcement should intensify from the Federal Trade Commission.

In 2021, the Federal Trade Commission cautioned companies on engaging in unfair or deceptive conduct, singling out the sale or use of biased algorithms. In clear fashion, the warning noted that companies must deploy AI lawfully, fairly, and with equity, or else the FTC may apply its enforcement authority under the FTC Act, the Fair Credit Reporting Act, and the Equal Credit Opportunity Act. The agency advised companies to (1) curb the deployment of AI models to areas identified as problematic, (2) verify that AI does not foster discrimination on the basis of race, gender, or any other protected class, (3) practice full transparency and invite independent evaluations, (4) avoid inflating claims about the device's capabilities and its ability to guarantee fair or impartial outcomes, and (5) disclose the source of all algorithmic data and the intended uses for the resulting outputs.

Workrapper surveillance and productivity scoring tools sold on the market leave both the software vendors and the employers they serve within the reach of possible FTC enforcement. By making this alert, the FTC permits companies to tighten their own Andre let lags in self-regulation be met with the FTC taking over for them.

Fortify capacities across workers' unions.

Workplace monitoring tools and productivity metrics can serve to crush union efforts at their outset and to erode the safeguards that unions are able to secure. In order to safeguard workers' rights, unions must strengthen their own internal capacities and capabilities..

According to workers' rights scholar Dr Colclough, unions must build their understanding of various digital technologies—as well as the commands given to artificial intelligence and algorithmic systems—and promptly overhaul their approaches, devising more effective collaboration across international borders "to make sure that all workers, irrespective of their work arrangements, enjoy equal social and fundamental rights". In systems that offer advantages to employers and to workers alike, the formulation and oversight of those algorithms ought to involve workers' representatives alongside the developers.

Unions ought to likewise leverage their expertise to aid both NLRB

and FTC in the execution of their enforcement duties. Unions are well positioned to supply NLRB with information about employers that deploy surveillance technologies and, consequently, are mandated to submit Surveillance Reports. Trade unions could also advise the FTC on firms that fail to deploy "AI in a truthful, fair, and equitable manner."

Unions may also request the EEOC and The Office of Federal Contract Compliance Programs (an arm of the U.S. Department of Labor) to supply tailored opinion letters to clarify the law around worker surveillance and productivity-scoring algorithms. These opinion letters may help illuminate and delineate lawful practices and applications.

No set of principles, nor any risk-management framework, should therefore confer legitimacy upon algorithmic systems that breach fundamental human rights and human dignity. Such systems ought not to be introduced into practice in the first instance. Conversely, systems that bolster workers' conditions, outputs, safety and well-being while giving employers their own advantages must be developed, operated, and overseen in full accordance with those safeguards.

Financial Sector Compliance: Recordkeeping, Surveillance, and Privacy Tensions

Regulatory Imperatives and Surveillance Drivers

In the financial sector, surveillance of employee communications is not a matter of managerial discretion—it is a statutory obligation.

In the U.S., **SEC Rule 17a-4** (broker-dealers) and **Rule 204-2** (Registered Investment Advisers) require firms to **archive all business-related electronic communications** for fixed retention periods—typically 5–6 years—in tamper-proof formats like WORM (Write-Once-Read-Many). This includes emails, instant messages, collaboration-tool chats, and even voice over IP calls if business content is discussed.

Critically, regulators interpret "business-related" broadly. So-called **off-channel communications**—including SMS, WhatsApp, Signal, and personal email—fall within the recordkeeping scope if used for business purposes. The SEC has clarified that it does not matter whether the device or account is employer-issued; the trigger is the content and context of the communication.

Failure to capture these channels has become a high-stakes compliance hazard. Since 2021, enforcement penalties have surged:

- Over **$1.6 billion** in fines between 2021–2023 for failures to retain off-channel communications.
- An additional **$81 million** in early 2024 actions.
- Cumulative SEC/FINRA penalties in this area exceeded **$2.8 billion** over 2022–2023.

These figures illustrate how the compliance mandate cascades down to employees, many of whom now work in hybrid or remote contexts where personal devices blur with professional duties.

Global Parallels

This is not uniquely American.

- **UK Financial Conduct Authority (FCA)**: Under the Senior Managers & Certification Regime and MiFID II, FCA-regulated firms must record and store all relevant communications, including mobile calls, texts, and messaging apps, for at least five years.
- **EU MiFID II**: Requires investment firms to record telephone conversations and electronic communications relating to transactions—capturing even those that do not lead to execution.
- **Hong Kong Securities and Futures Commission (SFC)**: Requires licensed corporations to record all client orders and relevant communications, with minimum retention periods.

In each of these jurisdictions, the underlying principle is the same: **regulatory traceability** outweighs employee privacy where business conduct is concerned.

Surveillance Infrastructure and Policies

These obligations have pushed firms to build comprehensive surveillance infrastructures:

- **Automated capture systems**: integrated with email servers, collaboration platforms (Teams, Slack), and mobile device management (MDM) tools.
- **Lexicon and AI-based monitoring**: scanning communications for keywords linked to compliance risk (e.g., insider information, market manipulation).
- **Archival systems** with redundancy, encryption, and tamper-proofing for audit readiness.
- **Supervisory dashboards** enabling compliance teams to review flagged communications in near-real time.

Regulators like FINRA and the SEC's Division of Examinations urge firms to regularly **audit** communication channels, **update policies** to include new apps, and **train employees** on compliant communication methods.

Despite this, a Reuters survey found **63% of financial institutions are not actively monitoring personal messaging apps**, and only **27%** are actively investing in upgrading surveillance capabilities—leaving significant compliance exposure.

Employee Privacy and Employment Consequences

The intensity of this monitoring erodes privacy in several ways:

- **Personal device spillover**: Employees may be compelled to install corporate monitoring apps or avoid using personal devices for any work-related purpose.
- **Credential restrictions**: New York's **A836 law** prohibits employers from demanding personal account credentials—potentially clashing with the SEC's expectation that firms capture all relevant communications.
- **Career sanctions**: Non-compliance can trigger "for cause" termination, **compensation clawbacks**, and for broker-

dealers, a damaging **Form U-5** filing that signals misconduct to future employers.

Conclusion and Recommendations:

n conclusion, this research reveals that digital surveillance in the workplace—once a sector-specific or high-security measure—has become a ubiquitous feature of modern employment across industries, geographies, and work arrangements, particularly in the wake of the COVID-19 pandemic's acceleration of remote and hybrid work. The technological capacity to monitor, record, and analyze employees' activities has outpaced the development of coherent, enforceable privacy protections, creating a persistent imbalance between employer oversight and worker autonomy. Indeed, in the financial industry, round-the-clock surveillance of communications has proven necessary to comply with the SEC Rule 17a-4 and FINRA record keeping rules with more than 2.8 billion of fines in two years (20222023). In the gig economy, though, platform algorithmic monitoring based on routes, acceptance rates, performance indicators (in real time, and with little or no transparency or effective appeal) creates an algorithmic Taylorism, in which work is divided into small, monitored tasks, and denies formal employment responsibilities. Other jurisdictions have been struggling with how to define the scope of legal monitoring courts and regulatory authorities greater freedom to monitor when it comes to determining the scope of legal monitoring- dividing line Cases with similar attributes in the European Court of Human Rights Barbulasco v. Romania confirmed that staff members have a reasonable expectation of privacy with regards to personal communications, regardless of their being worked on a work-issued device, whereas the New York Civil Rights Law 52-c and the Ontario Bill 88 explicit notice are provided in terms of electronic surveillance. However, in other countries (including Pakistan and India), where there has been no substantive legislation on privacy in the workplace, the terms of the employment contract are usually the only guidelines on controlling the surveillance measures and the wording thereof of primary importance. The consequences of this legal patchwork are very serious: without statutory restrictions, overbroad clauses enabling sweeping monitoring capabilities can be added to employment contracts by the employer in question, preventing the employee the possibility of asking questions without repercussions. The dangers of such freewheeling are multi-fold as research has shown that constant scrutiny has been known to decrease job satisfaction in employees by up to 75 percent and increase turnover intention rates by 50 percent in addition to cooling collective action as the same surveillance of the online community and union activities can be monitored. A danger in reducing these harms yet maintaining legitimate business and compliance needs is the use of a multi-layered preventive approach recommended by this research. Primarily, employers ought to take up the privacy-by-design approach in both contracts and policies

and explicitly indicate the purpose, scope, methods, and retention of monitoring, as well as deciding that it be relative against the risks undertaken. Employment contracts must not be open ended with the catch all provision but must be specified as to which systems and what contexts fall subject to monitoring, and avoidocracy personal devices unless employees sign up volunteer work use, and rights to access and challenge monitoring information should be acknowledged as part of employment policies. Second, governments should require Privacy Impact Assessments (PIAs) or Data Protection Impact Assessments (DPIAs) to be institutionalized, and worker representatives in relevant cases should be consulted to increase trust and legitimacy. Third, legislation needs to be updated to address regulatory gaps: in the U.S. the archaic Electronic Communications Privacy Act (ECPA) needs to be updated to match rrealities in cloud computing and mobile messaging; in Pakistan and India the Personal Data Protection Bill (PDPB) and the Digital Personal Data Protection Act (DPDPA) need to be enacted immediately to introduce baseline obligations such as purpose limitation and data minimization in the work place. Fourth, policymakers must incorporate into national labor laws provisions of "Right to Disconnect" already present in France, Australia, Portugal and others to strengthen work-life domains and curtail after-work surveillance. Fifth, reforms specific to the industry are necessary: in the financial sector regulators must look at moderate compliance frameworks which serve the interests of the investor community but do not enter abortive Into non-work communications whereas in gig economy, the platforms must be forced to reveal the algorithmic decision-making criteria, make performance data religiously available to workers and ensure that the existence of a reasonable appeal process against automated decisions.

Sixth, civil society and labor groups should take a role in the education and awareness of workers on their rights, attestation of abuses and encouragement of sousveillance avenues that individuals can use to watch and criticise unjust ways, tools like Turkopticon or GigSense are worker led and only require payment to use. Seventh, international collaboration to establish privacy norms ought to be sought, leveraging the power of GDPR to even out principles of legality, necessity, proportion and transparency within individual jurisdictions, and enforcement regimes that keep pace with technological roll out. Perhaps, the question is how to provide a system of governance a synthesized mixture of statutory protection, contract efficiency, use of technology and culture, which can balance the real interests of the employer to enforce productivity and compliance requirements and security and the basic rights as an employee, to dignity, autonomy, and to a life that is shared privately. It is not just a legal requirement but a business one: the Harvard Business Review among others has continually found that workplaces that are rich in trust produce better results

than those that are big on surveillance in terms of innovation, retention and overall productivity. An employment contract must be the absolute protecting layer and pattern that is able to provide a clearer picture of the rights and obligation, in addition to indicating an intent to maintain ethical monitoring. Governments should make sure that regulation can keep up with the rate of technological advancement rather than falling behind as previously with the introduction of 24/7 GPS tracking or keystroke logging services being introduced as standard after they already become accepted before laws could be written to protect against it. Employers can appreciate that over-surveillance can create reputation risks, risk of legal damages, and employee alienation and all due to the loss of the productivity it is intended to accomplish. And workers--both conventionally employed, remotely employed, and platform-based workers--need the tools, understanding, and laws to claim their rights in the face of spreading surveillance environments. Through their incorporation in the policy, law and practice, one can be able to navigate a direction into a future of work where technology complements, instead of undermining the intonement of trust on which the relationship of employment is built.

References

Sellers C. The market revolution. Oxford: Oxford University Press; https://scholar.google.com/scholar_lookup?title=The%20market%20revolution&author=C%20Sellers&publication_year=1991&

Snyder B. The Disrupted Workplace: Time and the Moral Order of Flexible Capitalism. Oxford: Oxford University Press; 2016. https://scholar.google.com/scholar_lookup?title=The%20Disrupted%20Workplace:%20Time%20and%20the%20Moral%20Order%20of%20Flexible%20Capitalism&author=B%20Snyder&publication_year=2016&

Barbaro, M.: The rise of workplace surveillance: is your productivity being electronically monitored by your bosses? New York Times. https://www.nytimes.com/2022/08/24/podcasts/the-daily/workplace-surveillance-productivity-tracking.html

Cyphers, B., Gullo, K.: Inside the invasive, secretive “Bossware” tracking workers. Electronic Frontier Foundation. https://pmc.ncbi.nlm.nih.gov/articles/PMC10026198/?utm_source=chatgpt.com#CR22

Weber, J.: Should companies monitor their employees' social media? Wall Street Journal.https://www.wsj.com/articles/should-companies-monitor-their-employees-social-media-1399648685

Ajunwa, Ifeoma: Algorithms at work: productivity monitoring applications and wearable technology as the new data-centric research agenda for employment and labor law 63 St. Louis. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247286

Vogell, H.: Rent going up? One company’s algorithm could be why. ProPublica. https://www.propublica.org/article/yieldstar-rent-increase-realpage-rent

Scherer, M., Brown, L.X.Z.: Warning: Bossware may be hazardous to your health. Center for Democracy and Technology. https://cdt.org/wp-content/uploads/2021/07/2021-07-29-Warning-Bossware-May-Be-Hazardous-To-Your-Health-Final.pdf

Manokha I. Surveillance, panopticism, and self-discipline in the digital age. Surveill. Soc. 2018 doi: 10.24908/ss.v16i2.8346. https://scholar.google.com/scholar_lookup?journal=Surveill.%20Soc.&title=Surveillance,%20panopticism,%20and%20self-

Kelly, K.: The Pinkertons have a long, dark history of targeting workers. Teen Vogue. https://www.teenvogue.com/story/who-were-the-pinkertons

Bernhardt, A., Kresge, L., Suleiman, R.: Data and algorithms at work: the case for worker technology rights. Center for Labor Research and Education, University of California, Berkeley.https://laborcenter.berkeley.edu/data-and-algorithms-at-work/

Wolford, M. (2025). Is your employer watching you?: Invasive employee surveillance in the modern era. North Carolina Journal of Law & Technology, 26(4), 617. https://journals.law.unc.edu/?s=Article+5

Smith, J., & Doe, A. (2023). The long shadow of workplace surveillance. *Stanford Social Innovation Review*. https://idronline.org/contributor/stanford-social-innovation-review/?utm_source=Google&utm_medium=Grants&utm_campaign=Dalit_History_06&gad_source=1&gad_campaignid=22591559224&gbraid=0AAAADCozDy_tl4WLvwMtPMXQm-nkYd1K&gclid=CjwKCAjwtfvEBhAmEiwA-DsKjhIwzwH0ZB9oKLTa0Rm0JxbA--cFijoKO8zV76WPn_NWolq1Mu3rbBoC3IYQAvD_BwE

Australian Government. Fair Work Ombudsman. https://www.fairwork.gov.au/

U.S. Senate, Subcommittee on Employment and Productivity, of the Committee on Labor and Human Resources: Marc Rotenberg and Gary T. Marx testimony for Proposed S. 516 The Privacy for Consumers and Workers Act of 1991. https://web.mit.edu/gtmarx/www/labor_hr_testimony.pdf (2022). Accessed 1 Mar 2023

European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012PC0011

Human Impact Partners: The Public Health Crisis Hidden in Amazon Warehouses. Oakland, CA (2021)

Tomczak, D.: Your boss is watching you. Is that OK? American Psychological Association podcast. https://www.apa.org/news/podcasts/speaking-of-

psychology/workplace-surveillance(2019). Accessed 1 Mar 2023