Surveillance and Algorithmic Management at Work: Capabilities, Trends, and Legal Implications

Adam Molnar, PhD
Assistant Professor
Sociology and Legal Studies
University of Waterloo

MARCH 2025

Contents

Disclaimer

This report was commissioned by the Office of the Information and Privacy Commissioner of Ontario (IPC) and is intended to synthesize emerging literature on surveillance and algorithmic management at work. The report is for informational purposes only and it should not be relied upon as a substitute for the legislation itself or as legal advice. The views reflected within the report are not necessarily those of the IPC. It does not bind the IPC, which may be called upon to independently investigate and decide upon an individual complaint or appeal based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this report, visit the IPC's website at **www.ipc.on.ca**.

Acknowledgements

The author gratefully acknowledges Chris Irwin, Krystle Shore, and Danielle Thompson for their valuable assistance in preparing this report.

Executive summary

Surveillance is a deeply entrenched aspect of organizational management. In the modern workplace, it has evolved into "management's ability to monitor, record and track employee performance, behaviours and personal characteristics in real time … or as part of broader organizational processes."[1] Surveillance can take many forms, from monitoring employee productivity, tracking online or device activity, drug testing, or even using hiring algorithms in recruitment processes before employment even officially begins.

While workplace surveillance is often justified by expectations of enhanced productivity, loss prevention, and security, it raises serious concerns about privacy, worker autonomy, and human rights in the increasingly digital workplace. As a management technique, surveillance directly serves the goals of business owners and managers: identifying both positive and negative deviations from managerially determined performance and behavioral standards.[2] While it can be used for safety, training, policy compliance, and cybersecurity, a disproportionate amount of workplace monitoring aims to control workers and increase productivity.[3] This aligns with 'scientific management' (Taylorism), an Industrial Revolution-era strategy focused on breaking down work processes into smaller elements. This managerial approach encourages close monitoring, analysis, and control to maximize efficiency and extract the greatest value from the labour process (including workers' behaviour) or to provide protection or direction.[4]

While scientific management itself is not new, its integration with digital surveillance tools, algorithms, and artificial intelligence (AI) within a densely networked technological environment significantly amplifies data collection. Such monitoring and automated management can routinely extend beyond the workplace, intruding upon workers' private lives. Workplace surveillance, while granting managers visibility into work processes, relies on technologies and processes of organizational datafication that blur work-life boundaries and negatively impact workers' privacy, psycho-social well-being, discretion, autonomy, and human rights.

The following review provides:

1. An overview of the range of technologies (and their capacities) being used for the purposes of workplace surveillance and employee monitoring today and considers the future evolution of these technologies as techniques of workplace management.
2. A review of a diversity of workplace environments and the different kinds of surveillance technologies that are being used to monitor different classes of workers in these environments.
3. An overview of the scholarly peer-reviewed research that documents harms and impacts of surveillance on employees (i.e., notably including mental health, loss of autonomy, alienation, and discriminatory effects).

1 Ball, K. (2010). Workplace surveillance: An overview. Labor History, 51(1), 87-106.

2 Sewell, G. (2021). Surveillance: A Key Idea for Business and Society (1st ed.). Routledge, 63.

3 Ball, K., Electronic Monitoring and Surveillance in the Workplace, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-43340-8, doi:10.2760/5137, JRC125716.

4 Ajunwa, I. (2020). The "black box" at work. *Big Data & Society*, 7(2), 1-6.

4. Four emerging and ongoing major trends that have implications for individuals' or communities' privacy rights at work.
5. A legal overview of how employee privacy is protected in Canada (Federally, British Columbia, Alberta, Quebec, and Ontario), the U.S. (California, Illinois, New York), the U.K., and Europe.

The report is organized as follows. **Section I** documents the range of workplace surveillance technologies that enable continuous, real-time monitoring of location, activity, biometrics, and even emotions, both at work and beyond. This section offers an easy-to-reference table for each technology, highlighting:

- Specific capabilities of each technology.
- Breadth of potentially accessible information.
- A brief identification of legal implications based on the scope of gathered information, highlighting Ontario's definitions of personal and personal health information, and the distinction between work-related and non-work-related data.
- Reference to major vendors or providers of each technology or system.

Section II examines the widespread integration of workplace monitoring and automated management across various economic sectors and industries. It delves into specific sectors, including retail, manufacturing, office and administration (particularly in remote/hybrid work), healthcare, warehousing, delivery, transportation, and platform work. The section analyzes the types of technologies, their underlying rationales, and the unique contexts within each setting, emphasizing the emerging privacy considerations in each environment.

Section III provides a comprehensive overview of scholarly peer-reviewed research on the impacts of workplace surveillance and automated management on employees, showing how it can impact mental health and well-being, autonomy and dignity, trust in the workplace, as well as the risks that are posed for individual and collective human rights.

Section IV highlights four critical trends in workplace monitoring and automated management that have implications for individuals' or communities' privacy rights at work. Specifically, they include: the ongoing datafication of organizations and employee visibility, and the strain placed on current regulatory effectiveness; the intensification of automated / algorithmic management; wearable devices and biometric technologies in the workplace; and the ongoing use of employee monitoring applications (EMAs) in office and administrative settings.

Finally, **Section V** provides a comprehensive legal review of workplace surveillance and employee privacy in Canada (covering the *Privacy Act*, PIPEDA, provincial laws in B.C., Alberta, Quebec, and Ontario, and the proposed Federal Bill-C27 — the CPPA and AIDA), followed by a targeted review of how employee privacy is protected in a range of other jurisdictions including the U.S. (California, Illinois, and New York), U.K. (U.K. GDPR), and Europe (AI *Act*, EU Rules on Platform Work). Based on this analysis, the section concludes with key attributes for a robust model that protects workers' rights in the digital workplace.

Notes on terminology and scope

In this report, the terms surveillance and monitoring are used interchangeably, as are the terms automated management and algorithmic management. While the concept of workplace surveillance is widely used in this report, it's important to understand that work often occurs across various spaces and occurs through interconnected technological networks. Therefore, while the term workplace surveillance may be used, it is in reference to surveillance of workplace activities rather than on a geographically defined workplace. Similarly, while this report often refers to surveillance technologies in the singular, it is important to recognize that workplace monitoring also often occurs through combined uses of technologies and data to facilitate more detailed analysis of employee activities. Due to space constraints, this report does not address conventional performance review practices (such as document-logged evaluations) or surveillance that is carried out by employees on other employees within the work environment (for a discussion of this topic, see Palm, 2009).[5] Finally, this report uses the term employees to encompass all types of employment, including full-time, part-time, temporary/casual, and self-employed individuals.

Section I: Workplace monitoring technologies

The data-driven reorganization of work has been accompanied by an associated introduction of new management models. These models leverage data to plan and organize workloads, predict worker behavior, monitor and influence employee actions, surveil workers, direct tasks, provide job assistance, and even fully automate tasks.[6] The transformation towards a data-centric workplace relies on various technologies that collect, store, and analyze data about workplace operations as well as employees. Such a constant flow of data, including workers' location, behaviors, thoughts, and feelings, can be used to enhance existing processes and, in some cases, even replace employee and managerial functions.

One of the key challenges in defining the appropriate use of surveillance technologies within extensive data-driven organizational management models is determining if, and how, the scope of data collection intrudes on employees' privacy by gathering sensitive personal information (PI) or personal health information (PHI). The following table provides a (non-exhaustive) overview of a common range of technologies employed for workplace surveillance and algorithmic management. It includes a brief account of their capabilities, the potential breadth of accessible information, whether (under Ontario legislation) this information relates to the definition of personal information or health information,[7] and some examples of products in each technological category.

5 Palm, E. (2009). Privacy expectations at work—What is reasonable and why? *Ethical Theory and Moral Practice*, 12, 201-215.

6 Aloisi, A., & De Stefano, V. (2022). Your boss is an algorithm: artificial intelligence, platform work and labour. Bloomsbury Publishing; Ball, K. (2022). Surveillance in the workplace: past, present, and future. *Surveillance and Society*.

7 Please see Appendix A for more detailed information on the definitions of PI and PHI in the employment context.

Technology	Description and capabilities	Breadth of potentially accessible information	Personal information or personal health information i.e., can exceed workplace activities)	Vendor technologies
Device activity monitoring Employee Monitoring Applications (EMAs)				Teramind, Controlio, Clever Control, StaffCop, ActivTrak, Hubstaff, WorkTime, Veratio, Kickidler, Insightful
Keystroke logging	Records all keystrokes on a device	Keystrokes, usernames, website addresses, passwords, work as well as private text/document communications, patterns of behaviour	PI and PHI	EMAs with keystroke logging include Hubstaff, Controlio, CleverControl
Keystroke activity	Tracks keyboard activity	Keyboard "metadata" regarding activity to detect user status	No, depending on collected metadata	EMAs with keystroke activity (but no logging) includes ActivTrak, Worktime
Mouse activity	Tracks mouse movements, clicks, hovers (often web-based).	Mouse coordinates, clicks, scrolling, hover time, elements interacted with (i.e., data associated with device interactions)	PI and PHI	EMAs with mouse activity include MouseKey Recorder, Time Doctor
Image / video capture	Range of tech (webcams to CCTV). Features include motion detection, facial recognition, time/ location metadata.	Images, video, timestamps, location (if enabled), includes 'incidental' 3rd party collection.	PI and PHI	EMAs with video capture include KickIdler, Veratio, Interguard, Controlio (includes FRT), and Teramind
Internet monitoring	Monitors internet activity at various levels. Tracks user website activity, including searches, IP addresses (i.e. sites visited), as well as other communication content.	URLs, IP addresses, search terms, metadata, communication content	PI and PHI	All EMAs listed above (with different degrees of features for internet monitoring)

Technology	Description and capabilities	Breadth of potentially accessible information	Personal information or personal health information i.e., can exceed workplace activities)	Vendor technologies
Email monitoring (content and metadata)	Monitors email activity, potential to read content.	Email addresses, subject lines, timestamps, metadata, potentially direct interception of email content / communications	PI and PHI	Mix between productivity monitoring and security purposes. Productivity monitoring EMAs that monitor email include Teramind, Interguard, and Email Analytics Security applications relating to email security include companies such as Mimecast, Cisco, or Proofpoint
File management monitoring	Tracks file actions (creation, modification, deletion, access). For productivity, security, etc	File names, paths, timestamps, access logs, file types, potentially contents	Could rise to level of PI if it includes geo-locational information in a remote-work environment	Microsoft Office 365
Facial recognition technology-enhanced image capture	Uses software to analyze images/ video, identifying individuals by comparing facial features to a database. Allows for real-time or stored image/video surveillance	Image of face, biometric data derived from the image, associated database records (if a match is found)	PI and PHI	EMAs such as Controlio and timerack.com (for attendance and time tracking). Applications relating to purposes of authentication and security also use FRT, such as Intel and Sine.co (Honeywell)
Social media monitoring	Tracks and analyzes an individual's activity on social media platforms. This may include posts, comments, likes, shares, and connections	Public social media content, social networks, expressed opinions and interests, potentially private messages if accessible	PI and PHI	All EMAs listed above

Technology	Description and capabilities	Breadth of potentially accessible information	Personal information or personal health information i.e., can exceed workplace activities)	Vendor technologies
Audio recording	Captures audio (personal devices or targeted surveillance). Potential for voice print identification	Raw audio, timestamps, potentially location data, audio metadata	PI and PHI	Verint and NICE systems for voice-print identification. For productivity monitoring often part of EMA w/ video capability Flexispy.com includes standalone audio record feature
Call recording	Records audio of phone/VOIP calls. Potential uses include customer service and surveillance	Audio of conversations, phone numbers, timestamps, call metadata	PI and PHI	NICE.com, Verint, Calabrio EMA flexispy.com includes standalone call monitoring
Video surveillance	Broad range of video capture (security cameras to large networks). Can have motion detection & facial recognition	Video recordings, timestamps, potentially location data, video metadata	PI and PHI	Honeywell, IBM, Securitas
GPS / geo-locational technologies	Monitors individual / vehicle movements — tracks physical location using GPS on smartphones, dedicated trackers, or data from cell towers/Wi-Fi signals,creates detailed location histories.	Precise location data (latitude/ longitude), timestamps, movement patterns, and potential identification of places of interest (home, work, etc.)	PI and PHI	Mobilepunch.ca, B2Field, Telus Fleet management, RAM Tracking, TitanGPS, Azuga
RFID technologies / key card Technologies	Uses radio-frequency identification for tracking and access control. RFID tags in cards/objects transmit unique identifiers, sensed by readers with varying ranges	Unique ID numbers associated with cards/tags, timestamps, location of RFID readers (access points), and potentially linked personal data	PI and PHI	Avigilon, BTI Group, Securitas

Technology	Description and capabilities	Breadth of potentially accessible information	Personal information or personal health information i.e., can exceed workplace activities)	Vendor technologies
Wearable devices	Broad range of technologies (including smartwatches, fitness trackers, other sensors) Collect health data, track location, monitor activity. Some devices may record images, audio, or enable communication	Highly variable – heart rate, step counts, location data, sleep patterns, potentially image/audio/ communications depending on the device	PI and PHI	Apple Watch, Fitbit, Garmin, ViSafe (wearable ergonomic sensors), RealWear, Eleksen, Oura
Biometric monitoring	Uses unique physical characteristics for identification, access control, or health/behavior monitoring. Includes drug testing	Fingerprint scans, facial recognition data, voiceprints, potentially DNA (drug testing), behavioral biometrics (gait, typing patterns, etc.)	PI and PHI	EMAs listed above, including Controlio that use FRT Wearable tech listed above collect biometric information Access control companies listed above, but also includes HID Global, Daon Inc.
Internet of things in the Workplace	Sensors, smart devices, and connected equipment to optimize operations, track assets, and even monitor employee behavior.	Location data, equipment usage patterns, environmental data (temperature, etc.), potentially biometric data if sensors incorporate those (facial recognition cameras, etc.)	PI and PHI Highly dependent on sensor data and context of application.	Siemens industrial IoT, Johnson Controls, Cisco, GE Digital, Honeywell, IBM, Intel
Workplace messaging monitoring	Software analyzes content on company messaging platforms (Slack, etc.) to look for keywords, sentiment, security risks, and even compliance violations	Content of messages (text, potentially attachments), communication patterns (who talks to whom, timing of messages), sentiment analysis results.	PI and PHI	Aware

Technology	Description and capabilities	Breadth of potentially accessible information	Personal information or personal health information i.e., can exceed workplace activities)	Vendor technologies
AI hiring algorithms	Tools that analyze resumes, social media profiles, or candidate data from assessments to predict job fit or potential for success.	Varies depending on the specificity of the tool: Resume data, social media content, results of vendor' algorithmic scoring, potentially protected characteristics (inferred race, age, etc.)	PI and PHI	HireVue, Talenture, Fetcher, Humanly, Findem

Section II: Contexts and rationales

Workplace surveillance and algorithmic management are complex issues involving diverse technologies, motivations, and impacts across workplaces. These systems vary in the roles they target, the monitoring methods employed, and the justifications used. This section elaborates on the previously discussed typology of workplace monitoring technologies, exploring in further detail their connections to distinct workplace settings and the rationales and applications that make up workplace monitoring (the subsequent section expands on this context to document the impacts on worker experiences). To identify sectors, Statistics Canadas (StatCan) North American Industry Classification System (NAICS) Canada 2022 Version 1.0 is used.[8] Importantly, a single business entity may operate within multiple sectors. For instance, a retail trade establishment which is vertically integrated to include both warehousing and transportation/delivery. Where relevant, this analysis will break down different activities and contexts, but please note that these categories are solely meant to help guide the discussion.

Retail sector

The retail trade sector is vast and encompasses a broad range of establishments that render an array of products and services to the public. They encompass so-called 'brick and mortar' establishments as well as internet retail through online platforms or direct selling — covering a range of services such as clothing, food and hospitality, entertainment, and many others. Across these contexts, modern retail is a "data-intensive business" with extensive information management practices that collect and coordinate vast amounts of fine-grained data "at the level of individual products, staff, and customers" that span "Enterprise Resource Planning (ERP), Supply Chain Management (SCM) and Customer

8 StatsCan. 2024. North American Industry Classification System (NAICS) Canada 2022 Version 1.0. https://www23.statcan.gc.ca/imdb/p3VD.pl?Function=getVD&TVD=1369825

Relationship Management (CRM)."[9] Scientific management is reproduced in the big data-driven retail sector, albeit through interlinked technological innovations that greatly intensify the extent and frequency of monitoring and algorithmic decision-making, and by extension, worker control.[10]

There is a lack of research into the breadth and depth of how retail businesses in Canada have adopted workplace technologies. StatCan does not collect any nationally representative data on the diffusion of AI or other adoption of information technology / digitalization of Canadian business environments, which could include vital information on the use of workplace technologies to monitor or manage workers across all sectors, including retail.[11] In the U.S. researchers facing similar constraints from the American Bureau of Statistics (ABS) have turned to collect data directly from retail workers. One survey, conducted in late 2022, revealed the prevalence of worker surveillance and automation in the retail and food services industry. Recruiting 10,000 workers employed at 140 different U.S.- based employers (through Facebook ad sampling), they found that "80% of workers reported their employers use technology to monitor the quality of their work, and nearly 25% [of] workers reported that it was at least somewhat likely that their employers were monitoring them outside of work.[12]

In practical terms, workplace surveillance in the retail sector can be divided into two main contexts. First, workplace monitoring can be more directly worker focused — driven by the logic scientific management and applying techniques of surveillance that quantify and evaluate workers for the purposes of productivity / performance monitoring. This type of surveillance typically entails the application of traditional physical managerial oversight, technologies to document attendance, as well as computer or other digital device monitoring, such as EMAs. Second, monitoring in the workplace is also directed toward purposes such as ERP, SCM, and CRM. It is against this broader context that technologies that may be designated for one purpose are subsequently repurposed for employee monitoring. For instance, commercial retail stores using video surveillance for crime control, loss prevention or safety are often repurposed for managerial purposes to monitor and discipline the individual performance of employees.[13] Similarly, point-of-sale systems, originally designed for facilitated sales transactions (to facilitate ERP and SCM) are

9 Evans, L., & Kitchin, R. (2018). A smart place to work? Big data systems, labour, control and modern retail stores. *New Technology, Work and Employment*, 33(1), 44-57, pg. 45; Chopra and Meindl, (2012). Supply Chain Management: Strategy, Planning and Operation. Pearson.

10 Evans, L., & Kitchin, R. (2018). A smart place to work? Big data systems, labour, control and modern retail stores. *New Technology, Work and Employment*, 33(1), 44-57.

11 Collecting data on employer use of technologies for workplace monitoring in future surveys through StatCan and other provincial agency surveys in the future is essential to document and understand the adoption, use, and impacts of employee monitoring technologies in the workplace.

12 For overview of their survey recruitment and data collection methods, see: Schneider, Daniel, and Kristen Harknett. 2019. "Consequences of Routine Work-Schedule Instability for Worker Health and Well-Being." American Sociological Review 84 (1): 82–114. https://doi.org/10.1177/0003122418823184.; Harknett, Kristen and Daniel Schneider. 2023. "Workplace Technology and Worker Well-Being" UCSF California Labor Laboratory conference on Surveillance, Monitoring, & Data Gathering in Contemporary Employment held virtually on May 2-3, 2023. https://youtu.be/majQcpUrmsY.

13 Ball, K. (2002). Elements of surveillance: A new framework and future directions. Information, Communication & Society, 5(4), 573-590 (p.578); McCahill, M., Norris, C. (1999). Watching the Workers: Crime, CCTV and the Workplace. In: Davies, P., Francis, P., Jupp, V. (eds) Invisible Crimes. Palgrave Macmillan, London. https://doi.org/10.1007/978-1-349-27641-7_8; Ditton, J. (2000). Crime and the City, The British Journal of Criminology, Volume 40, Issue 4, September, Pages 692–709, https://doi.org/10.1093/bjc/40.4.692

repurposed (or are purposefully enhanced through technological function-creep) to record how many returns are processed by sales workers, which is evaluated in relation to broader quotas on 'normal' number of returns to facilitate discipline.[14] And finally, the introduction of remote employee safety devices (ESDs) in the hospitality industry (including in Canada) as a means to provide safety and security from sexual assault against hotel staff, while offering a layer of protection, can simultaneously provide real-time locational data on employees that managers use to track them.[15] The devices have also been found to have weak security — potentially putting additional sensitive user data at risk.[16]

Moreover, in another example of the privacy risks of the tech-intensive workplace, the increasing use of facial recognition technology (FRT) in retail outlets not only poses risks to consumers, but also indirectly to employees. A number of stores, including Home Depot, Walmart, and Macy's are (or have in the past) used facial recognition technology for "asset protection services."[17] US-based drug store giant Rite-Aid recently settled with the Federal Trade Commission (FTC) to cease their use of facial recognition technology in their stores for five years because their technology was used against customers without consent and was biased toward disproportionately identifying "women, Black, Latino or Asian people" on "numerous occasions" as being "likely to engage" in shoplifting.[18] The FRT system would then alert employees to place these individuals under enhanced surveillance and to impose store bans. In Canada, Canadian Tire's use of FRT for the purposes of 'customer and employee safety' over a duration of three-years was found by the BC OIPC to violate BC PIPA given their failure to notify and obtain consent from shoppers. The BC OIPC report goes on to say that the stores still would not have been able to demonstrate a reasonable purpose for collection and use.[19] The report does not explicitly mention the corollary impacts on employee privacy. While the full extent of FRT technology use in the retail sector is Canada is unknown, the risks of employee's biometric information being 'incidentally' collected by private third-party vendors remains a significant area of concern for employee privacy.

Manufacturing

The manufacturing sector includes a range of work activities that relate to the creation or assembly of component parts into manufactured goods and often take place in plants, factories, or mills. Given the direct relationship to manual labour in a manufacturing setting, a range of surveillance technologies are often applied in accord with the precepts of scientific management for the purposes of employee attendance, time and productivity

14 Nguyen, A. (2021) The constant boss: work under digital surveillance. Data & Society Institute. https://apo.org.au/sites/default/files/resource-files/2021-05/apo-nid312352.pdf

15 Lindzon, J. (2020, June 02). Security flaws threaten 'panic buttons' meant to protect hotel workers. *Fast Company*. https://www.fastcompany.com/90458034/security-flaws-threaten-panic-buttons-meant-to-protect-hotel-workers

16 Lindzon, J. (2020, June 02). Security flaws threaten 'panic buttons' meant to protect hotel workers. *Fast Company*. https://www.fastcompany.com/90458034/security-flaws-threaten-panic-buttons-meant-to-protect-hotel-workers

17 Hill, K. (2023, March 10)." Which Stores Are Scanning Your Face? No One Knows." The New York Times. https://www.nytimes.com/2023/03/10/technology/facial-recognition-stores.html

18 Bhuiyan, J. (2023, December 20)." Rite Aid facial recognition misidentified Black, Latino and Asian people as 'likely' shoplifters." The Guardian. https://www.theguardian.com/technology/2023/dec/20/rite-aid-shoplifting-facial-recognition-ftc-settlement

19 Office of the Information and Privacy Commissioner for British Columbia. (2023). Canadian Tire Associate Dealer's Use of Facial Recognition Technology. OIPC. https://www.oipc.bc.ca/investigation-reports/3785

monitoring, access control, health and safety monitoring, and for tracking the movement of employees and goods throughout the production process. While forms of monitoring in the manufacturing sector are perhaps some of the oldest 'modern' examples of workplace surveillance (the use of video surveillance, attendance access control technology, and direct managerial supervision of the shop-floor), the turn to so-called just in time (JIT) or total quality management (TQM) manufacturing systems at the turn of the 1990s,[20] combined with enhanced technologization of the manufacturing sector, has deepened interconnections between machinery and the workforce.[21] Brynjolfsson and McEhlerhan (2016) note in their study that reliance on data-driven decision making in U.S. manufacturing nearly tripled from 2005–2010, ushering in a so-called "data-driven revolution in management" in the manufacturing sector.[22]

The technologization (and datafication) of manufacturing environments facilitates novel forms of employee monitoring and management, consolidating into intensified, data-centric managerial control over the workplace. Most commonly, worker-specific surveillance in the manufacturing sector accords with rationales of productivity as well as health and safety. In the latter, the permeation of sensor technologies to detect unsafe working environments (e.g., to monitor fatigue levels or detect harmful exposures) is furthered through the use of wearable technologies.[23] When these technologies are designed to collect ambient data that relates to the broader work environment (e.g., air quality), they can be used toward ensuring optimal safety outcomes with little impact on employee privacy. However, when these technologies are directly connected to persons as the primary source of data collection — whether through wearable technologies or the use of mobile apps on smartphones to manage smart machinery, a deeper understanding of their design, data capture (i.e., if it includes biometric vitals such as heart rate, steps / geolocation, and/or fatigue levels), and broader end-user visibility over the network becomes critical for understanding the attendant risks they may pose to worker privacy. Further research on the surveillance and privacy risks of smart manufacturing environments is necessary.

Historically, employee reactions to monitoring in the global manufacturing supply chain have stressed the need to improve working conditions, including resisting unreasonable forms of monitoring. In one example from the 'pre-digital era' in 1978, a walkout of over 200 unionized workers (190 of them immigrant women) at Toronto textile factory occurred in opposition to management's installation of nine security cameras at the workplace, including one that was placed outside the women's washroom.[24] Today, workers routinely employ digital tools in the workplace, such as mobile device communications, to participate

20 Delbridge, R., Turnbull, P., & Wilkinson, B. (1992). Pushing back the frontiers: management control and work intensification under JIT/TQM factory regimes. New Technology, work and employment, 7(2), 97-106.

21 Müller, S., Baldauf, M., & Seeliger, A. (2022). Ubiquitous Machinery Monitoring-A Field Study on Manufacturing Workers' User Experience of Mobile and Wearable Monitoring Apps. Proceedings of the ACM on Human-Computer Interaction, 6(MHCI), 1-22.

22 McAfee, A., Brynjolfsson, E., (2012) Big data: the management revolution. Harvard Business Review. 90(10): 60-68.

23 Kritzler, M., Backman, M., Tenfalt, A., and Michahelles, F. (2015). Wearable technology as a solution for workplace safety. MUM '15: Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia, 213–217. https://doi.org/10.1145/2836041.2836062.

24 Godden, M. (2020). Contesting Big Brother: Legal Mobilization against Workplace Surveillance in the Puretex Knitting Company Strike, 1978–1979. Labour / Le Travail, 86, 71–98. https://www.erudit.org/en/journals/llt/2020-v86-llt05768/1074473ar/

and advocate in labour rights and unionization.[25] As manufacturing environments become increasingly smart and more densely interconnected, these examples highlight the critical importance of meaningful privacy protections for workers in the manufacturing sector (and more broadly).

Office and administrative work

Employee monitoring in office and administrative environments is often justified by several reasons, including to monitor employee productivity,[26] to maintain cyber and information security,[27] to facilitate the use of artificial intelligence (AI) technologies in the hiring process (i.e., recruitment),[28] and for analyzing employee (and project) behaviours and patterns to facilitate predictive decision making.[29] This section is inclusive of a broad range of NAIC sectors where administrative and information management duties are present, including finance, insurance, information and cultural industries, professional technical and scientific services, administrative support, and management).

Pre-work: The use of automated hiring tools for recruitment

Automated hiring tools are software applications and associated technologies designed to streamline the recruitment process. These tools include resume parsing software to screen and assess job candidate applications, applicant tracking systems (ATS) that manage recruitment workflows, and scoring systems that rank candidates based on specific criteria. Additionally, some tools feature video interview analysis software, which utilizes AI to interpret data provided during candidate interviews. This comprehensive suite of tools aims to optimize hiring efficiency and accuracy. However, these tools are known for containing bias and contributing to other discriminatory impacts.[30] Research into early attempts at regulating AI hiring algorithms in New York have shown that only a small fraction of companies are complying with obligations to notify applicants about their use of the algorithms, and to publish mandatory audit reports.[31]

---

25 Helmerich, N; Raj-Reichert, G; Zajak, S. (2021). Exercising associational and networked power through the use of digital technology by workers in global value chains. Competition and Change. 25 (2) 142 – 166.

26 Ravid, D. M., Tomczak, D. L., White, J. C., & Behrend, T. S. (2020). EPM 20/20: A review, framework, and research agenda for electronic performance monitoring. *Journal of Management*, 46(1), 100–126. https://doi.org/10.1177/0149206319869435

27 Elifoglu, I. H., Abel, I., & Taşseven, Ö. (2018). Minimizing insider threat risk with behavioral monitoring. Review of business, 38(2), 61-73.

28 Kelan, E. K. (2023). Algorithmic inclusion: Shaping the predictive algorithms of artificial intelligence in hiring. *Human Resource Management Journal*; Bongard, A. (2019). Automating talent acquisition: Smart recruitment, predictive hiring algorithms, and the data-driven nature of artificial intelligence. Psychosociological Issues in Human Resource Management, 7(1), 36-41; Hofeditz, L., Mirbabaie, M., Luther, A., Mauth, R., & Rentemeister, I. (2022). Ethics guidelines for using AI-based algorithms in recruiting: Learnings from a systematic literature review.

29 Kuziemski, M., & Misuraca, G. (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications Policy*, 44(6), 101976.

30 Fritts, Megan, and Frank Cabrera. "AI recruitment algorithms and the dehumanization problem." *Ethics and Information Technology* 23 (2021): 791-801.

31 Vigliarolo, B. (2024, January 23). Law designed to stop AI bias in hiring decisions is so ineffective it's slowing similar initiatives: New York's LL144 rated too broad, but researchers hope others can learn from that mistake. *The Register*. https://www.theregister.com/2024/01/23/nyc_ai_hiring_law_ineffective/

At-work: Call-centres as an early model of intensive workplace surveillance

Call centres are among the most familiar industries that are synonymous with extensive forms of data-driven monitoring and management. However, in recent times, call centres have been subject to more extensive forms of monitoring through industry-tailored technologies of employee monitoring such as Cogito, a software that delivers "real-time AI coaching." Cogito monitors call centre employee-customer conversations in real-time, analyzing the data through sentiment analysis, and provides immediate guidance on how employees can manage the calls. Managers have access to a customer experience score based on automatic tracking that "enables visibility into performance improvement."

The post-pandemic workplace surveillance transformation

Since the COVID-19 pandemic, office and administrative work has undergone one of the most significant transformations in workplace organization in the modern era. The move to remote and hybrid-work during- and post-pandemic is part of a three-fold process that blurs the conventional distinction between work and private life and raises distinct privacy concerns associated with the intensification of workplace monitoring and data collection beyond workplace activities and into private behaviours, thoughts, and emotions. First, the move to remote or hybrid work increased the scale of business activities being conducted from a personal / home environment. Current estimates find that about half of the U.S. workforce worked remotely at least one day a week as of December 2020.[32] Second, remote and hybrid work is now undertaken through a densely networked information communications environment where both work and personal devices can be used by multiple users on private / home internet networks, including by different family members or roommates for work, educational or schooling purposes, and personal uses.[33] This highlights one of the chief privacy concerns in the modern hybrid context — its intrusion into the domestic environment, including more intensive collection of information that extends beyond employment-specific task performance.[34] Third, compounding this development during this period, businesses have vastly expanded the use of digital tools to monitor worker activity. Evidence at the start of the pandemic indicated that global demand for EMAs had surged by 108 per cent in April 2020 and 70 per cent in May 2020 compared to 2019.[35]

Indeed, in the U.S., the New York Times found that 8 out of 10 of America's largest private employers use a form of productivity tracking tool.[36] A survey from Gartner Research

32 Brynjolfsson, E., Horton, J. J., Makridis, C., Mas, A., Ozimek, A., Rock, D., & TuYe, H. Y. (2023). How many Americans work remotely? a survey of surveys and their measurement issues (No. w31193). National Bureau of Economic Research.

33 Nurse, J. R., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021). Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy. In HCI International 2021-Posters: 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, Part III 23 (pp. 583-590). Springer International Publishing.

34 Nurse, J. R., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021). Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy. In HCI International 2021-Posters: 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, Part III 23 (pp. 583-590). Springer International Publishing.

35 Brynjolfsson, E. et al. (2020). COVID-19 and Remote Work: An Early Look at US Data. Survey Conducted by MIT. https://mitsloan.mit.edu/shared/ods/documents?PublicationDocumentID=6322

36 Kantor, J & Sundaram, A. (2022, August 14). The Rise of the Worker Productivity Score. Across industries and incomes, more employees are being tracked, recorded and ranked. What is gained, companies say, is efficiency and accountability. What is lost? *The New York Times*. https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html

found that large employers using employee monitoring software (EMAs) in the U.S. roughly doubled to 60 per cent since the start of the pandemic, going on to note that they expect this number to climb up to 70 per cent over the next three years.[37] Another survey found that 67% of North American employers with at least 500 employees or more used EMAs.[38] Express VPN notes in their own market survey that 78 per cent of employers report using EMAs "to track employee performance and/or online activity."[39] A poll of 1250 US employers by Digital.com in 2022 highlighted that "60% of companies with employees who work remotely use EMAs to track employee activity and productivity, and "88% of companies terminated workers after implementing the software."[40]

In Canada, Thompson and Molnar (2023) have conducted the only survey to date of Canadian businesses that focuses on the adoption of EMAs.[41] The survey (n=402) targeted sectors with a high-capacity for remote work as defined by StatCan (e.g., finance, insurance, education, professional / scientific and technical) in Ontario (60 per cent), BC (30 per cent), and Quebec (10 per cent).[42] The specific aims of the study were to gather data on the size, scope, purposes, rationales, barriers to adoption, and experiences of businesses surrounding the use of EMAs. The data showed an increase in the use of EMAs after the start of the pandemic (up roughly 22 per cent) compared with before the pandemic, with over half of the survey respondents (51.7 per cent) indicating that they used EMAs to monitor the workplace.[43] In line with other survey research (quoted above), EMAs are overwhelmingly adopted by large companies (47.5 per cent) (i.e., companies with 500 or more employees) and medium-large companies (23 per cent) (i.e., companies with 100-499 employees). Companies with 100 or fewer employees made up the remainder of survey with approximately 30 per cent (8.2 per cent 50-99, 11.7 10-49, and 10 per cent under 10 employees).

The main rationales provided by Canadian businesses adopting EMAs were to "protect sensitive company information" (91 per cent) and to "maintain general cybersecurity" (91 per cent).[44] The main stated uses of EMAs (i.e., not stated rationales, but actual applications after adoption) were to "manage employee productivity" (29 per cent), to "improve company

37 The Future of Employee Monitoring. (2024, April. 12). Gartner.com. https://www.gartner.com/smarterwithgartner/the-future-of-employee-monitoring

38 Ziegler, B. (2022, August 20). Should Companies Track Workers With Monitoring Technology? Employers can know when you're logged in, what you're typing and analyze your facial expressions. That raises all sorts of difficult questions. The *Wall Street Journal*. https://www.wsj.com/articles/companies-track-workers-technology-11660935634

39 Belton, E. (2023, March 10) 78% of employers engage in remote work surveillance: ExpressVPN survey finds Research into the remote workforce reveals unsettling insights on the extent to which employees are being surveilled by their employers and how it's impacting workers' job satisfaction, stress levels, and relationships with their employers. Express VPN. https://www.expressvpn.com/blog/expressvpn-survey-surveillance-on-the-remote-workforce/

40 Digital.com (2021, October 4). Employee Monitoring Statistics. https://web.archive.org/web/20231124064212/https://digital.com/employee-monitoring-statistics/

41 Thompson, D. E., & Molnar, A. (2023). Workplace Surveillance in Canada: A survey on the adoption and use of employee monitoring applications. Canadian Review of Sociology/Revue canadienne de sociologie, 60(4), 801-819

42 Deng, Z, Morissette, R & Messacar, D (2020) Running the economy remotely: potential for working from home during and after COVID-19 [Web log post]. Statistics Canada. Retrieved from: https://www150.statcan.gc.ca/n1/ pub/45- 28-0001/2020001/article/00026- eng.htm

43 Thompson, D. E., & Molnar, A. (2023). Workplace Surveillance in Canada: A survey on the adoption and use of employee monitoring applications. *Canadian Review of Sociology/Revue canadienne de sociologie*, 60(4), 801-819.

44 Thompson, D. E., & Molnar, A. (2023). Workplace Surveillance in Canada: A survey on the adoption and use of employee monitoring applications. Canadian Review of Sociology/Revue canadienne de sociologie, 60(4), 801-819.

efficiency" (21 per cent), and to "manage a remote workforce" (20 per cent).[45] When asked about the main barriers to the adoption of EMA use, respondents noted that they were "too privacy invasive" (29 per cent), that it can "undermine employer-employee trust relationships (25 per cent), and that laws surrounding their use are "unclear" (16 per cent).[46] Overall, the data show that many companies who did not view EMAs as a necessary part of workforce management before the COVID-19 pandemic have subsequently integrated them into their operations as a post-pandemic legacy effect. Moreover, the data show a disconnect between the rationales that businesses provide for acquiring EMAs (mostly cybersecurity) versus how they are applied in the workplace (mostly productivity monitoring). Interestingly, companies also appear to be aware of the invasiveness of EMAs (71 per cent) but are still opting to use the software in their business operations (52 per cent).[47]

In perhaps the only other Canadian survey in the private sector on the topic of EMAs, a 2022 Capterra survey shed light on the use and experiences of EMAs in Canadian workplaces from the perspective of workers.[48] Of the 752 employees surveyed, 35 per cent reported their companies used EMAs. The pandemic also influenced this trend — 28 per cent of companies had these tools in place beforehand, while 7 per cent were understood to have adopted them after the pandemic began.[49] However, a significant portion of respondents (47 per cent) indicated no EMAs were used at their workplace, and 18 per cent were unsure. When comparing this data to the survey from Thompson and Molnar (2023) it could be the case that many employees are unaware that their employer is using EMAs. From the employee perspective, the top perceived reasons for EMA use were boosting productivity (47 per cent), verifying work hours (25 per cent), and tracking workload (13 per cent).[50]

While EMAs represent some of the most invasive monitoring configurations, more mundane monitoring can occur through a range of enterprise technologies. For example, Microsoft's flagship software Office 365, while not an EMA, can be used for employee monitoring through access to file activity metadata. Recently, the use of Office 365 by the European Commission was found to violate GDPR because of its offshoring of data through its cloud system, a violation of regulations that require the Commission to mandate that personal data transferred outside of the European Union/European Economic Area (EEA) are afforded equivalent protection as within the EU/EEA.[51]

45 Thompson, D. E., & Molnar, A. (2023). Workplace Surveillance in Canada: A survey on the adoption and use of employee monitoring applications. Canadian Review of Sociology/Revue canadienne de sociologie, 60(4), 801-819.

46 Thompson, D. E., & Molnar, A. (2023). Workplace Surveillance in Canada: A survey on the adoption and use of employee monitoring applications. Canadian Review of Sociology/Revue canadienne de sociologie, 60(4), 801-819.

47 Thompson, D. E., & Molnar, A. (2023). Workplace Surveillance in Canada: A survey on the adoption and use of employee monitoring applications. Canadian Review of Sociology/Revue canadienne de sociologie, 60(4), 801-819.

48 It is important to note that Capterra is a private company that offers a software review and selection platform.

49 Anaya, T. (2022, May 30). Workplace surveillance: How do Canadians feel about employee monitoring? Capterra. https://www.capterra.ca/blog/2733/workplace-surveillance-employee-monitoring-software

50 Anaya, T. (2022, May 30). Workplace surveillance: How do Canadians feel about employee monitoring? Capterra. https://www.capterra.ca/blog/2733/workplace-surveillance-employee-monitoring-software

51 EDPS Press Release. (2024, March). European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies. https://www.edps.europa.eu/system/files/2024-03/EDPS-2024-05-European-Commission_s-use-of-M365-infringes-data-protection-rules-for-EU-institutions-and-bodies_EN.pdf

Healthcare and social assistances[52]

Employee monitoring practices in healthcare settings are diverse, encompassing various purposes, employees, and technologies. Biometrics and RFID-enabled identification badges are widely used for access control in protected medical facilities,[53] while video surveillance that tracks movement and behaviour of employees is also prevalent.[54] Also, EMAs may be used to monitor the devices of healthcare workers. EMA vendors openly market this capability and application, advertising their products to address overcharging in the rescue medical services industry.[55] [56] While research on device monitoring in the healthcare industry is limited, however, its use will likely remain relevant as remote delivery models like telehealth and mHealth (mobile health) technologies become more widespread.

Data-brokers and people intelligence platforms also facilitate employee monitoring in the healthcare sector, both before and after hiring. InfoMart, a U.S.-based vendor, boasts a "verified watchlist" solution for "continuous criminal monitoring" that integrates with HR management software such as Workday and PeopleSoft.[57] This real-time background screening technology service also includes a comprehensive search of potential job candidate's credit history and social media platforms that is designed to flag "workplace safety concerns: racism/intolerance, violence, potentially illegal activity, or sexually explicit material."[58] While this technology is advertised in the health context "to protect vulnerable populations," it is also broadly advertised for use across every business industry (and as such it could be included in any other sector discussed in this section).

Finally, caregiving staff are often subject to extensive levels of employee monitoring both directly by their employer in institutional settings and through mobile device monitoring when delivering remote services. Specifically, this includes in-facility, including in nursing home rooms, and other in-home surveillance technology, like sensors and trackers, that can collect worker behaviours.[59] In Sweden, homecare workers have been required to carry GPS-equipped mobile phones and are expected to communicate their location and visits.

---

52 This sector relates to establishments that are involved with "providing health care by diagnosis and treatment, providing residential care for medical and social reasons, and providing social assistance, such as counselling, welfare, child protection, community housing and food services, vocational rehabilitation and childcare, to those requiring such assistance." This includes EMTs and paramedics, hospital workers, nursing and residential care workers, as well as a range of social assistance workers in counselling, welfare, child protection and others. See NAICS 2024. (2023, June 1). North American Industry Classification System (NAICS) Canada 2022 Version 1.0. https://www23.statcan.gc.ca/imdb/p3VD.pl?Function=getVD&TVD=1369825&CVD=1369826&CPV=62&CST=27012022&CLV=1&MLV=5

53 Fisher, J. A., & Monahan, T. (2008). Tracking the social dimensions of RFID systems in hospitals. *International Journal of Medical Informatics*, 77(3), 176-183.

54 Khan, A., & Nausheen, S. (2017). Compliance of surgical hand washing before surgery: role of remote video surveillance. J Pak Med Assoc, 67(1), 92-96; Boyce, J. M. (2011). Measuring healthcare worker hand hygiene activity: current practices and emerging technologies. *Infection Control & Hospital Epidemiology*, 32(10), 1016-1028.

55 Worktime Case study. (2024, April 12). Worktime Respectful Employee Monitoring. https://www.worktime.com/7500-per-employee-per-year-is-saved-rescue-medical-services

56 Worktime Case study. (2024, April 12). Worktime Respectful Employee Monitoring. https://www.worktime.com/7500-per-employee-per-year-is-saved-rescue-medical-services

57 Informart.com. (2024, April 12). Strategic Partnerships We've partnered with the best to bring our clients superior screening service. https://www.infomart-usa.com/partners/

58 Informart.com. (2024, April 12). Social Media Searches: A compliant image of your candidate's social persona. https://www.infomart-usa.com/social-media-searches/

59 Berridge, C., Halpern, J., & Levy, K. (2019). Cameras on beds: The ethics of surveillance in nursing home rooms. AJOB empirical bioethics, 10(1), 55-62.

The data allows for a "minute-by-minute commissioning of care" by evaluating the amount of time spent at each visit and all transportation in between.[60] Critics have pointed out how this monitoring is used to intensify care labour by minimizing paid time while maximising the use of unpaid time.[61] Similarly, the adoption of similar geographic information technology to facilitate home healthcare delivery in Finland was criticized for its potential to track employees.[62] Overall however, more research is required to assess the extent and character of employee monitoring, particularly monitoring of those workers that may be required to be subject to on-device monitoring as part of mobile caregiving services.[63]

Transportation and warehousing

This sector includes establishments that facilitate the transportation of passengers and goods and the warehousing or storing of goods. In transportation, it can include long-haul trucking, courier, transit, package delivery, and ground passenger transportation such as taxis or rideshares. In warehousing, it includes workers that carry out tasks of managing warehouse inventory and collecting and packing retail orders for delivery.

Warehousing surveillance

Amazon warehousing and logistics are often regarded as the most intensive form of worker surveillance in warehousing.[64] With a global workforce of 1.54 million workers,[65] and over 40,000 employed in Canada,[66] the reach and impact of Amazon's automated surveillance management systems are substantial. Monitoring in Amazon warehouses is facilitated through radio frequency-enabled hand-held scanners that collect data about worker activities every second to evaluate performance against organizationally defined quotas. Workers are provided an individual rate quota at the start of each shift through which their tasks are subsequently measured by calculating so-called time off task (TOT). Any time that transpires between scans, time for bathroom visits, rest periods, travel within the sprawling warehouse after returning from breaks, "talking to another Amazon associate,"[67] or any other injuries or accommodations, may be defined as TOT. Managers routinely monitor these quotas and encourage workers to increase their productivity rates through "verbal warnings, warnings communicated through the scanner, visual warnings on a station

60 Palm, E. (2009). Privacy Expectations at Work—What is Reasonable and Why? Ethical Theory and Moral Practice 12 (2):201-215.

61 Moore, S., & Hayes, L. J. B. (2017). Taking worker productivity to a new level? Electronic Monitoring in homecare—the (re) production of unpaid labour. *New Technology, Work and Employment*, 32(2), 101-114

62 Voukko, R. (2007). Interdependence and control at work: social issues in transforming care work with mobile technology. Proceedings of ETHICOMP The Ninth International Conference, 621–632.

63 Overall, the importance of protecting healthcare professional's rights in the workplace extend to whistleblower protections, being able to report unethical or illegal activities without fear of retaliation or punishment.

64 Athena Coalition. (2022, June 29). In the Matter of Automated Worker Surveillance and Management Document Num. 2023–09353. https://drive.google.com/file/d/1h90_EuSK8JKoq3oK3ks_aqO9LnoTW5hW/view

65 Amazon (2022). Amazon 2022 Annual Report. https://s2.q4cdn.com/299287126/files/doc_financials/2023/ar/Amazon-2022-Annual-Report.pdf

66 AboutAmazon.com. (2023, June 23). Amazon's economic impact in Canada: How we're investing in local communities. https://www.aboutamazon.com/news/policy-news-views/amazons-economic-impact-in-canada-2023

67 Gurley, L. (2022, June 2). Internal Documents Show Amazon's Dystopian System for Tracking Workers Every Minute of Their Shifts: The documents provide new clarity about a much-talked-about but until now opaque process Amazon uses to punish associates it believes are wasting time. Vice.com. https://www.vice.com/en/article/5dgn73/internal-documents-show-amazons-dystopian-system-for-tracking-workers-every-minute-of-their-shifts

screen, printouts, and large screens of everyone's rates for comparative purposes."[68] Any accumulation of TOT is also used to discipline workers on an ongoing basis throughout the year (for example, accumulations of 30 minutes of TOT on three separate days in a one-year period can lead to termination), leading to reported instances of Amazon workers skipping water and bathroom breaks out of fear of discipline or termination.[69]

Transportation and delivery surveillance

Amazon's last-mile delivery model subcontracts small local delivery service partners (DSPs) as part of their retail operation. DSPs are ostensibly independent businesses (in terms of legal contract with Amazon) that manage employment of roughly 275,000 drivers. These DSPs subsequently employ drivers who are subject to extensive surveillance and automated management that monitors driver and vehicle behaviour through driver facing cameras, smartphone apps, and GPS tracking, and that dictates delivery routes, sets productivity quotas and delivery deadlines.[70] [71] Drivers are also obligated to agree to "biometric consent terms as a condition of employment that authorize constant real-time surveillance and performance evaluations through AI-enhanced cameras.[72] These cameras, one vendor of which is Netradyne Driver-i[73], record the road and driver constantly, collecting vehicle telemetry data about speed, location, and actions on the road. These technologies are known to make inaccurate conclusions about driver performance even though they are used by Amazon to enforce disciplinary penalties.[74] Notably, drivers as part of the UPS-Teamsters negotiated road facing cameras only as part of their 2023 contract negotiations.[75]

Other forms of performance managing through fleet management systems in transportation sector relate to the trucking industry. Mandated electronic logging devices (ELDs) are digital systems that collect data about truckers' activities, particularly hours of operation, to limit the number of driving hours that exceed regulatory limits. Designed to prevent over-work and/or fatigue, ELDs create a digital record through geo-location and other detailed vehicle

68 Athena Coalition. (2022, June 29). In the Matter of Automated Worker Surveillance and Management Document Num. 2023–09353. https://athenaforall.org/news/worker-organizations-and-allies-respond-to-white-house-request-for-input-on-automated-worker/, p 5.

69 Gurley, L. (2022, June 2). Internal Documents Show Amazon's Dystopian System for Tracking Workers Every Minute of Their Shifts: The documents provide new clarity about a much-talked-about but until now opaque process Amazon uses to punish associates it believes are wasting time. Vice.com. https://www.vice.com/en/article/5dgn73/internal-documents-show-amazons-dystopian-system-for-tracking-workers-every-minute-of-their-shifts

70 Eidelson, J. & Day, M. (2021, May 5). Driver's don't work for Amazon but company has lots of rules for them. The Detroit News. https://www.detroitnews.com/story/business/2021/05/05/drivers-dont-work-amazon-but-company-has-lots-rules-them/4955413001/; This program has been criticized in the US as a way to deny status as joint-employer while still requiring intensive forms of monitoring and automated management. See Leon, L. (2023, May 4). Teamsters Begin Major Amazon Fight. *American Prospect*. https://prospect.org/labor/2023-05-04-teamsters-begin-major-amazon-fight/.

71 It is also worth noting that drivers are subject to significant degrees of monitoring by smart doorbell cameras at the so-called 'digital doorstep'. See Nguyen, A., & Zelickson, E. (2022). At the Digital Doorstep: How Customers Use Doorbell Cameras to Manage Delivery Workers. Data & Society Research Institute (Oct 12, 2022).

72 Vincent, J. (2021, March 24). Amazon delivery drivers have to consent to AI surveillance in their vans or lose their jobs. The Verge. https://www.theverge.com/2021/3/24/22347945/amazon-delivery-drivers-ai-surveillance-cameras-vans-consent-form

73 https://www.netradyne.com

74 See Gurley, L. (2021, Sept 20). Amazon's AI Cameras Are Punishing Drivers for Mistakes They Didn't Make. *Vice Motherboard*. https://www.vice.com/en/article/88npjv/amazons-ai-cameras-are-punishing-drivers-for-mistakes-they-didnt-make

75 Cook, M. (2023, July 10). Teamsters Contract Prohibits Use of In-Cab Cameras. Arkansas Business. https://www.arkansasbusiness.com/article/teamsters-contract-prohibits-use-of-in-cab-cameras/

telemetry—that are expected to be less vulnerable to tampering than paper logs.[76] Levy (2023) shows how information collected through ELDs are accessible to both government regulators, insurers, freight brokers, as well as trucking firms — serving as a workplace monitoring technology that affords a significant amount of real-time data collection about truckers' activities across a wide range of organizations.[77] ELDs, however, are also known to be subject to a wide variety of strategies that undermine their assumed effectiveness.[78]

Platform work and the gig economy

Platform work is a more recent workplace surveillance context that is widely regarded for the consistency, intensity, and invasiveness of monitoring.[79] Described as being subject to a form of "end-to-end employee surveillance,"[80] workers in the platform economy are typically short-term subcontractors that carry out tasks facilitated through a digital labour platform.[81] The work often varies in terms of whether it is performed exclusively online (in an online labour market like Amazon's Mechanical Turk), or whether it is carried out by a person facilitating mobile services in-person (such as food delivery or transportation such as Uber). In Canada, StatCan estimates that 871,000 people have taken on gig work in their main job in the fourth quarter of 2022 (which may or may not include paid work on a platform) and that in December 2023, 468,000 people aged 15 to 69 years indicated they had worked through a digital platform or app to earn income in the previous 12 months and were paid by the platform for their work.[82]

Platform workers are subject to intensive data collection that facilitates opaque, algorithmic decision-making regarding future work allocation, remuneration levels, and potential rewards.[83] Extensive personalized data, including worker performance metrics, behaviors, location, vehicle telemetry (if applicable), and customer feedback, is used to both nudge workers towards desired actions and evaluate their performance (often publicly disclosed via the app interface). Failure to conform to these algorithmic expectations can result in the restriction of future opportunities for the worker. The lack of transparency, potential for algorithmic bias, and limitations on worker autonomy in platform work raise urgent ethical and regulatory questions.[84]

---

76 Levy, K. 2023. Data Driven. Princeton University Press: NJ.

77 Levy, K. 2023. Data Driven. Princeton University Press: NJ.

78 Levy, K. 2023. Data Driven. Princeton University Press: NJ.

79 Jarrahi, M. H., Sutherland, W., Nelson, S. B., & Sawyer, S. (2020). Platformic management, boundary resources for gig work, and worker autonomy. Computer supported cooperative work (CSCW), 29, 153-189; Newlands, G. (2022). The algorithmic surveillance of gig workers: Mechanisms and consequences. In *The Routledge Handbook of the Gig Economy*. Routledge. 64-73.

80 Ball, K. (2021). Electronic Monitoring and Surveillance in the Workplace, Publications Office of the European Union, Luxembourg ISBN 978-92-76-43340-8, doi:10.2760/5137, JRC125716, pg. 6.

81 While difficult to define in general terms, Ball (2021, see previous note) references some defining features noted by Eurofound, namely that: paid work is organized through an online platform, three parties are involved: the online platform, the client and the worker, the aim is to carry out specific tasks or solve specific problems, the work is outsourced or contracted out, jobs are broken down into tasks, services are provided on demand.

82 StatsCan. (2023, March 4). Defining and measuring the gig economy using survey data: Gig work, digital platforms, and dependent self-employment. StatsCan. https://www150.statcan.gc.ca/n1/daily-quotidien/240304/dq240304b-eng.htm

83 Pignot, E. (2023). Who is pulling the strings in the platform economy? Accounting for the dark and unexpected sides of algorithmic control. *Organization*, 30(1), 140-167.

84 Muller, Z. (2019). Algorithmic harms to workers in the platform economy: The case of Uber. Colum. JL & Soc. Probs., 53, 167.

Section III: Understanding the impacts of workplace surveillance

While the impacts of employee monitoring have been documented for some time, the recent intensification of data-driven surveillance and automated decision-making marks a significant shift in organizational control. The following section presents the results of a comprehensive systematic literature review that documents the impacts of electronic surveillance on employees, noting how monitoring can erode autonomy and dignity, negatively influence worker mental health and wellbeing, undermine work performance, and lead to worker alienation and a loss of employee trust.[85]

Employee autonomy and dignity

Several studies have examined the impact of employee monitoring on worker autonomy. Surveys conducted by Smith et al. (1992), Jeske and Santuzzi (2015), and Liao and Chun (2016), for example, indicate that monitored employees perceive less control over their work compared to their non-monitored counterparts.[86] This trend is also supported by field research (e.g., ethnographic research and case studies) (e.g., Westin, 1992).[87]

Additionally, early employee monitoring (EM) work by Chalykoff and Kochan (1989)[88] found that workplace monitoring can limit supervisor autonomy, thus limiting their ability to effectively develop their employees. Gerten, Beckmann, & Bellman (2019),[89] in their empirical study of workplace information and communication technologies (ICTs), found that managers are more affected by both workplace monitoring practices and levels of employee autonomy than the employees being monitored.

Other research has found practices do not significantly impact employee autonomy and empowerment (e.g., Martin, Wellen, & Grimmer, 2016).[90] Survey research by Martin and colleagues (2016) shows a positive psychosocial work environment has a more substantial influence on employee attitudes than monitoring practices and that such environmental factors can mitigate any negative impacts of employee surveillance.[91] Similarly, Aiello

85 This literature review is part of a scholarly paper in progress from Molnar, A. and Shore, K. A systematic review of employee monitoring research: Toward a relational understanding of workplace surveillance practices.

86 Smith, M. J., Carayon, P., Sanders, K. J., Lim, S. Y., & LeGrande, D. (1992). Employee stress and health complaints in jobs with and without electronic performance monitoring. Applied ergonomics, 23(1), 17-27; Jeske, D., & Santuzzi, A. M. (2015). Monitoring what and how: psychological implications of electronic performance monitoring. *New Technology, Work and Employment*, 30(1), 62-78; Liao, E. Y., & Chun, H. (2016). Supervisor monitoring and subordinate innovation. Journal of Organizational Behavior, 37(2), 168-192.

87 Westin, A. F. (1992). Two key factors that belong in a macroergonomic analysis of electronic monitoring: Employee perceptions of fairness and the climate of organizational trust or distrust. *Applied Ergonomics*, 23(1), 35-42.

88 Chalykoff, J., & Kochan, T. A. (1989). Computer-aided monitoring: Its influence on employee job satisfaction and turnover. *Personnel Psychology*, 42(4), 807-834.

89 Gerten, E., Beckmann, M., & Bellmann, L. (2019). Controlling working crowds: The impact of digitalization on worker autonomy and monitoring across hierarchical levels. *Jahrbücher für Nationalökonomie und Statistik*, 239(3), 441-481.

90 Martin, A. J., Wellen, J. M., & Grimmer, M. R. (2016). An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours. *The International Journal of Human Resource Management*, 27(21), 2635-2651.

91 Martin, A. J., Wellen, J. M., & Grimmer, M. R. (2016). An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours. *The International Journal of Human Resource Management*, 27(21), 2635-2651.

and Svec (1993) found that providing participants with a sense of control over their work conditions can alleviate the negative effects of monitoring (e.g., felt stress, reduced task performance).[92] Moreover, Bakewell and colleagues (2018) found through their interview research that contemporary remote monitoring practices may enhance employee autonomy. Relatedly, Barrenchea-Méndez, Ortín-Ángel, and Rodes (2016) propose that increased autonomy in the workplace necessitates heightened monitoring practices to oversee the increased levels of employee discretion.[93] Gerten, Beckmann, and Bellman (2019) argue that ICT technologies can simultaneously facilitate workplace monitoring and promote employee autonomy through decentralized workplace practices.[94]

Some literature highlights the factors that moderate the impact(s) of EM on employee autonomy. For instance, Borg and Arnold III (1997) conducted an empirical examination of workplace drug testing and reveal that formal monitoring practices are more prevalent in environments characterized by low normative respectability and weak social ties. Their work implies that individuals with higher level of workplace respect and stronger social connects face less monitoring and subsequently less social control.[95]

The impact of employee surveillance on employee autonomy can impact multiple areas of work life. Survey research by Bernstrøm and Svare (2017) found that employees' perceptions of control is associated with felt trust, and that felt trust mediates the (negative) relationship between monitoring and an employee's motivation as well as monitoring and an employee's sense of mastery at work.[96] Douthitt and Aiello (2001) conducted a laboratory experiment, manipulating levels of employee participation in, and control over, monitoring practices, and found that higher levels of employee participation and control in monitoring practices is associated with higher employee job satisfaction and increased workplace performance;[97] Backhaus' more recent (2019) meta-analytic review of workplace monitoring literature supports these claims, suggesting that a "participatory approach" to monitoring enhances job satisfaction and monitoring acceptance, and generally contributes to an improved workplace environment.[98]

The ramifications of reduced employee autonomy (as an impact of EM) also extend beyond the workplace. Charitsis (2019) discusses how corporate wellness programs — which

92 Aiello, J. R., & Svec, C. M. (1993). Computer monitoring of work performance: Extending the social facilitation framework to electronic presence 1. *Journal of Applied Social Psychology*, 23(7), 537-548.

93 Barrenechea-méndez, M.a., Ortín-Ángel, P. and Rodes, E.C. (2016), Autonomy and Monitoring. Journal of Economics & Management Strategy, 25: 911-935. https://doi.org/10.1111/jems.12164

94 Gerten, E., Beckmann, M., & Bellmann, L. (2019). Controlling working crowds: The impact of digitalization on worker autonomy and monitoring across hierarchical levels. *Jahrbücher für Nationalökonomie und Statistik*, 239(3), 441-481.

95 Borg, M. J., & Arnold III, W. P. (1997, September). Social monitoring as social control: The case of drug testing in a medical workplace. In *Sociological Forum* (Vol. 12, pp. 441-460). Kluwer Academic Publishers-Plenum Publishers.

96 Bernstrøm V, Svare H. Significance of Monitoring and Control for Employees' Felt Trust, Motivation, and Mastery. *Nordic Journal of Working Life Studies*. 2017;7(4):29-49 http://dx.doi.org/10.18291/njwls.v7i4.102356

97 Douthitt, E. A., & Aiello, J. R. (2001). The role of participation and control in the effects of computer monitoring on fairness perceptions, task satisfaction, and performance. Journal of applied psychology, 86(5), 867.

98 Valencia-Forrester, F., Patrick, C. J., Webb, F., & Backhaus, B. (2019). Practical Aspects of Service Learning Make Work-Integrated Learning Wise Practice for Inclusive Education in Australia. *International Journal of Work-Integrated Learning*, 20(1), 31-42.; Ravid, D. M., Tomczak, D. L., White, J. C., & Behrend, T. S. (2020). EPM 20/20: A review, framework, and research agenda for electronic performance monitoring. *Journal of Management,* 46(1), 100-126; Jensen, J. M., & Raver, J. L. (2012). When self-management and surveillance collide: Consequences for employees' organizational citizenship and counterproductive work behaviors. *Group & Organization Management,* 37(3), 308-346; McNall, L. A., & Stanton, J. M. (2011). Private eyes are watching you: Reactions to location sensing technologies. *Journal of Business and Psychology*, 26, 299-309.

increasingly rely on the deployment of self-tracking technologies (e.g., Fitbits) — can compromise employee autonomy; seemingly voluntary participation in such programs (which can have deleterious effects for employees when, for example, data is shared with insurance companies) are driven by unspoken workplace pressures that inhibit employees from opting out.[99] Relatedly, Manley and Williams (2022) emphasize that information about employees that is gathered through contemporary surveillance technologies tends to define employees through standardized "numerical language"; their interviews with monitored employees showed a culture of comparison that was "created through the open dissemination of quantifiable metrics and often in real time."[100] The authors emphasize that such practices have a detrimental effect on employee self-worth and serve "less as a motivational force and more so as a means to establish opinions imparted by the managerial hierarchy and demarcate those deemed essential to the successful functioning of the organization, enhancing feelings of insecurity surrounding employment and undermining a true sense of collaboration among employees".[101]

Theoretical perspectives frame monitoring practices as mechanisms of power. Ball and Wilson (2002) assert that monitoring technologies are "enmeshed with discourses which produce and reproduce relations of power and resistance in the workplace" and that as a result, "workers are made visible, classified, marked, constituted as workers and drilled as such."[102] Earlier work by Delbridge and colleagues (1992) shows that surveillance technologies in factory work entrenches managerial control and intensifies work (see also Cardon et al., 2021).[103] Kellogg and colleagues (2020) view algorithmic monitoring systems as instruments of control that obscure methods for securing capital from employee efforts.[104] Shapiro (2018) similarly points out that the entire "on-demand" economy is built upon subtle but pervasive "company strategies of arbitrage" that undercut worker autonomy;[105] empirical work by Wood et al. (2019) shows that, while the gig economy may appear to offer workers control over their work conditions, the reality is that algorithmic control, which "is central to the operation of online labour platforms,"[106] connects clients to "a largely unregulated global oversupply of labour" (p. 70) that often leads to gig-workers'

99 Charitsis, V. (2019). Survival of the (data) fit: Self-surveillance, corporate wellness, and the platformization of healthcare. *Surveillance & Society*, 17(1/2), 139-144.

100 Manley, A., & Williams, S. (2022). 'We're not run on Numbers, We're People, We're Emotional People': Exploring the experiences and lived consequences of emerging technologies, organizational surveillance and control among elite professionals. *Organization*, 29(4), 692-713.

101 Ibid, p. 16.

102 Ball, K. (2002). Elements of surveillance: A new framework and future directions. *Information, Communication & Society*, 5(4), 573-590. p.562

103 Delbridge, R., Turnbull, P., & Wilkinson, B. (1992). Pushing back the frontiers: management control and work intensification under JIT/TQM factory regimes. *New Technology, work and employment*, 7(2), 97-106; Cardon, P., Ma, H., Fleischmann, A. C., & Aritz, J. (2021). Recorded work meetings and algorithmic tools: Anticipated boundary turbulence.

104 Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. *Academy of management annals*, 14(1), 366-410.

105 Shapiro, A. (2018). Between autonomy and control: Strategies of arbitrage in the "on-demand" economy. *New Media & Society,* 20(8), 2954-2971.

106 Wood, A. J., Graham, M., Lehdonvirta, V., & Hjorth, I. (2019). Networked but commodified: The (dis) embeddedness of digital labour in the gig economy. *Sociology*, 53(5), 931-950, 70.

overwork and exhaustion (see also Jarrahi et al., 2020).[107] [108] Similarly, according to Sewell and Taskin (2015), while remote monitoring technologies may give employees a greater sense of felt autonomy, they also introduce new restrictions that extends managerial control into new (and previously unmonitored) spaces.[109]

Additionally, de Vaujany and colleagues (2021) summarize the negative impact of EM on employee autonomy in their introduction to a recent special journal issue on the topic of workplace surveillance and control.[110] The authors stress that our post-pandemic monitoring practices has contributed to "a new tension between autonomy and control, where technologies are promoting increased flexibility in terms of the time and space of work, at the same time as increasing [employee] control and surveillance."[111] However, the authors also point out that these "new work" circumstances have spawned "opportunities for workers and managers to develop creative tactics of resistance" (p. 688) to work surveillance/control practices (see also Ezzamel et al., 2001; Hafermalz, 2021; Sewell and Taskin, 2015).[112] [113] Moro and colleagues (2019) likewise point out the propensity for innovative surveillance technologies to embed workplace control practices while noting that the precise manifestation of control in these situations depends largely on the organizational environment and available forums for worker resistance (e.g., the presence of workers' unions).[114]

This comprehensive review of studies on employee monitoring and autonomy reveals a complex landscape where surveillance practices significantly impact workers' sense of control, autonomy, and dignity. The research consistently shows that increased monitoring can lead to perceptions of decreased autonomy among employees, influencing their motivation, job satisfaction, and overall workplace performance negatively. However, when monitoring practices are transparent, participatory, and integrate employee feedback, they may mitigate some of these negative effects. As Ball (2005) emphasizes, the power dynamics associated with monitoring often results in a nuanced interplay of control, resistance, and in this instance, adaptation by employees.[115] Overall, this cross-section of research underscores the importance for regulators to consider human factors in monitoring practices to support employee well-being.

---

107 Wood, A. J., Graham, M., Lehdonvirta, V., & Hjorth, I. (2019). Networked but commodified: The (dis) embeddedness of digital labour in the gig economy. *Sociology*, 53(5), 931-950, 70.

108 Jarrahi, M. H., Sutherland, W., Nelson, S. B., & Sawyer, S. (2020). Platformic management, boundary resources for gig work, and worker autonomy. *Computer supported cooperative work (CSCW),* 29, 153-189.

109 Sewell, G., & Taskin, L. (2015). Out of sight, out of mind in a new world of work? Autonomy, control, and spatiotemporal scaling in telework. *Organization studies,* 36(11), 1507-1529.

110 De Vaujany, F. X., Leclercq-Vandelannoitte, A., Munro, I., Nama, Y., & Holt, R. (2021). Control and surveillance in work practice: Cultivating paradox in 'new'modes of organizing. *Organization Studies*, 42(5), 675-695.

111 De Vaujany, F. X., Leclercq-Vandelannoitte, A., Munro, I., Nama, Y., & Holt, R. (2021). Control and surveillance in work practice: Cultivating paradox in 'new'modes of organizing. *Organization Studies*, 42(5), 675-695, 687.

112 De Vaujany, F. X., Leclercq-Vandelannoitte, A., Munro, I., Nama, Y., & Holt, R. (2021). Control and surveillance in work practice: Cultivating paradox in 'new'modes of organizing. *Organization Studies*, 42(5), 675-695, 687.

113 Ezzamel, M., Willmott, H., & Worthington, F. (2001). Power, control and resistance in 'the factory that time forgot'. *Journal of management studies, 38*(8), 1053-1079; Hafermalz, Ella. (2020). Out of the Panopticon and into Exile: Visibility and Control in Distributed New Culture Organizations. *Organization Studies*. 42. 017084062090996. 10.1177/0170840620909962; Sewell, G., & Taskin, L. (2015). Out of sight, out of mind in a new world of work? Autonomy, control, and spatiotemporal scaling in telework. *Organization studies*, 36(11), 1507-1529.

114 Moro, A., Rinaldini, M., Staccioli, J., & Virgillito, M. E. (2019). Control in the era of surveillance capitalism: an empirical investigation of Italian Industry 4.0 factories. *Journal of Industrial and Business Economics*, 46, 347-360.

115 Ball, K. (2005). Organization, surveillance and the body: Towards a politics of resistance. *Organization*, 12(1), 89-108.

Employee mental health and well-being

The impact of workplace monitoring on employee mental health and wellbeing has been extensively studied. Research clearly highlights the propensity for monitoring systems to induce or exacerbate employee stress, and to yield adverse impacts on psychological and social well-being. For instance, experimental studies by Schleifer, Galinsky, and Pan (1996) and Kolb and Aiello (1996) demonstrate increased mood disturbances (e.g., irritation, tension, dissatisfaction, boredom, and fatigue) among workers in monitoring conditions.[116] Survey work by Smith and colleagues (1992) demonstrates workplace monitoring adversely impacts employees' experiences of job stress, job strain, and psychological wellbeing.[117] More specifically, monitored employees reported higher levels of boredom, tension, anxiety, depression, anger, and fatigue — alongside related psychosomatic symptoms including headaches, heart palpitations, and gastro-intestinal disturbances — than those who did not experience workplace monitoring (Smith et al., 1992).[118] Deery, Iverson, and Walsh (2002) have linked monitoring to employee exhaustion and burnout.[119] Holman et al. (2006), in their survey research, conclude that high levels of employee monitoring can, over time, make employees more anxious and depressed.[120] Survey research by Roger, Smith, and Sainfort (1990) demonstrates the propensity for EM to have both direct and indirect impacts on employee wellbeing: while monitored employees reported a significantly higher level of psychological stress than those who are not monitored, they also reported higher levels of workload, fewer lulls between periods of heavy workload, poorer relationships with supervisors, lower levels of task meaningfulness, and higher perceptions of career/future ambiguity.[121] As the authors conclude, the impact of EM on employee stress "may be influenced by the monitoring system itself, or the service standards set by management, based on monitoring performance data" (Roger et al., 1990, p. 855).[122] Indeed, Carayon (1993) proposed an early conceptual approach to the study of EM that emphasizes the direct and indirect impact of monitoring on worker stress.[123]

While early research predominantly shows a negative impact of EM on employee emotional wellbeing, Holman, Chissick, and Totterdell (2002) stress that such effects are not straightforward and are contextually mediated. In their survey work, the authors show that EM can have enhanced impacts on employee wellbeing when it is used for

116 Schleifer, L. M., Galinsky, T. L., & Pan, C. S. (1996). Mood disturbances and musculoskeletal discomfort: Effects of electronic performance monitoring under different levels of VDT data-entry performance. International Journal of Human-Computer Interaction, 8(4), 369-384; Kolb, K. J., & Aiello, J. R. (1996). The effects of electronic performance monitoring on stress: Locus of control as a moderator variable. *Computers in Human Behavior*, 12(3), 407-423.

117 Amick III, B. C., & Smith, M. J. (1992). Stress, computer-based work monitoring and measurement systems: A conceptual overview. *Applied Ergonomics*, 23(1), 6-16.

118 Amick III, B. C., & Smith, M. J. (1992). Stress, computer-based work monitoring and measurement systems: A conceptual overview. *Applied Ergonomics*, 23(1), 6-16.

119 Deery, S., Iverson, R., & Walsh, J. (2002). Work relationships in telephone call centres: Understanding emotional exhaustion and employee withdrawal. *Journal of Management studies,* 39(4), 471-496.

120 Holman, D., Chissick, C., & Totterdell, P. (2002). The effects of performance monitoring on emotional labor and well-being in call centers. *Motivation and Emotion*, 26, 57-81.

121 Rogers, K. J., Smith, M. J., & Sainfort, P. C. (1990, October). Electronic performance monitoring, job design and psychological stress. In *Proceedings of the Human Factors Society Annual Meeting* (Vol. 34, No. 12, pp. 854-858). Sage CA: Los Angeles, CA: SAGE Publications.

122 Rogers, K. J., Smith, M. J., & Sainfort, P. C. (1990, October). Electronic performance monitoring, job design and psychological stress. In *Proceedings of the Human Factors Society Annual Meeting* (Vol. 34, No. 12, pp. 854-858). Sage CA: Los Angeles, CA: SAGE Publications, 855.

123 Carayon, P. (1993). Job design and job stress in office workers. *Ergonomics*, 36(5), 463-477.

constructive purposes (i.e., employee feedback) rather than as a security-based or punitive measure.[124] The authors note that this positive effect of monitoring on employee wellbeing (when monitoring is deployed for constructive purposes) occurs vis-à-vis job satisfaction. In contrast, Henderson and colleagues' (1998) experimental research shows that electronic monitoring negatively impacts worker physiological stress regardless of whether it is deployed for performance or security purposes.[125] Davidson and Henderson's experimental research shows that electronic performance monitoring can increase positive moods for workers when they are completing relatively easy workplace tasks, but also that the monitoring exacerbates workers' negative mood states when they are completing difficult tasks.

Other early research suggests that external factors can mitigate the negative impact of monitoring on employee wellbeing. For instance, Westin's (1992) fieldwork links intense workplace monitoring practices to increases in employee stress, while highlighting how employee perceptions regarding the fairness of the monitoring practice, and the overall climate of trust within the workplace environment, can reduce the stress employees experience because of the monitoring.[126] Conversely, Westin points out that the impact of monitoring on employee stress is exacerbated when the monitoring is perceived by employees as unfair or as breaching their expectations of trust in the workplace. Aiello and Kolb's experimental research shows employees experience more anxiety because of monitoring when they have low perceived levels of control over the monitoring conditions; as a result, the authors suggest that organizations should include workers in the design and implementation of workplace monitoring systems.[127]

Some contemporary literature claims employee monitoring can be a useful tool for monitoring and addressing employee experiences of distress in the workplace: work by Bromuri and colleagues (2021) suggests employers can deploy workplace surveillance systems specifically to identify instances of employee emotional distress; Gärtner and colleagues (2013) suggest their surveillance tool can be used by employers to encourage employees to seek emotional support.[128] However, Chartsis (2019) — in their discussion of the rise of employee wellness initiatives that rely on surveillance technologies (and especially self-tracking devices like Fitbits) — warns that such surveillance technologies and practices can, ironically, impede employee wellbeing due to, for instance, related workplace pressure for employees to conform to standardized conceptions of "wellness"

124 Holman, D., Chissick, C., & Totterdell, P. (2002). The effects of performance monitoring on emotional labor and well-being in call centers. *Motivation and Emotion*, 26, 57-81.

125 Henderson, R., Mahar, D., Saliba, A., Deane, F., & Napier, R. (1998). Electronic monitoring systems: an examination of physiological activity and task performance within a simulated keystroke security and electronic performance monitoring system. *International Journal of Human-Computer Studies*, 48(2), 143-157.

126 Westin, A. F. (1992). Two key factors that belong in a macroergonomic analysis of electronic monitoring: Employee perceptions of fairness and the climate of organizational trust or distrust. *Applied Ergonomics, 23*(1), 35-42.

127 Aiello, J. R., & Svec, C. M. (1993). Computer monitoring of work performance: Extending the social facilitation framework to electronic presence 1. *Journal of Applied Social Psychology,* 23(7), 537-548.

128 Bromuri, S., Henkel, A. P., Iren, D., & Urovi, V. (2021). Using AI to predict service agent stress from emotion patterns in service interactions. J*ournal of Service Management, 32*(4), 581-611; Gärtner, F. R., Ketelaar, S. M., Smeets, O., Bolier, L., Fischer, E., van Dijk, F. J., Nieuwenhuijsen, K. & Sluiter, J. K. (2011). The Mental Vitality@ Work study: design of a randomized controlled trial on the effect of a workers' health surveillance mental module for nurses and allied health professionals. *BMC Public Health*, 11, 1-13.

or the fact that such programs tend to replace more human-led and interactive employee wellness programs.[129]

While many employee monitoring application vendors suggest device-level surveillance systems can enhance employee wellbeing and flexibility,[130] academic scholars clearly emphasize that, such practices have the capacity to adversely affect employee wellbeing by blurring the boundaries between employee work and home life (and thus increasing work-related demands and stressors while detracting from downtime and familial/support relationships) (e.g., Adisa, Gbadamosi, and Osabutey, 2017).[131] Bakewell and colleagues (2018) looked at how remote performance monitoring systems affect mobile workers and found that, while these remote monitoring systems may enhance autonomy and collaboration among workers, they also intensify the workload and role responsibility for those being monitored, thus "render[ing] any gain of greater job control disputable"[132].

A considerable body of literature is more concrete regarding the negative impacts of contemporary electronic monitoring. For instance, research regularly shows employee monitoring decreases employee job satisfaction, affective commitment, and perceptions of self-efficacy which may then have negative repercussions for (employee) health and psychosocial wellbeing. Shin's (2019) interviews with service employees who are subjected to mystery shopping (wherein someone hired to evaluate customer service poses as a shopper) shows that the scrutiny of such practices exacerbate already-high levels of service employee stress and related issues like sleep disturbances, low levels of self-esteem, and even cardiovascular disease.[133] Manley and Williams (2022) examined the lived experiences of emerging organizational surveillance technologies on professionals in organizations, showing that, "while it was apparent that the inability to escape the gaze of the organization was prominent in the minds of the [monitored professionals], and the enhanced scrutiny of surveillance technologies permeated their everyday lives, heightened levels of distrust, anxiety, fear and insecurity were perceived as the most common consequences arising from an environment guided by performance metrics and data surveillance devices."[134] The authors also found that such systems promote worker anxiety regarding their own productivity and how the monitoring data may be interpreted by their managers (and related consequences of managerial interpretations).

Such findings are in line with work by work by Van Oort (2019), who shows that "flexibility" offered through workplace surveillance technologies in retail settings tends to operate as a form of digital control that exacerbates worker insecurity, especially for

129 Charitsis, V. (2019). Survival of the (data) fit: Self-surveillance, corporate wellness, and the platformization of healthcare. *Surveillance & Society*, 17(1/2), 139-144.

130 See for example, ActivTrak (2024) The Benefits of Employee Monitoring for Work-from-Home Arrangements, Blog https://www.activtrak.com/blog/employee-monitoring-work-from-home/

131 Adisa, T. A., Gbadamosi, G., & Osabutey, E. L. (2017). What happened to the border? The role of mobile information technology devices on employees' work-life balance. *Personnel Review*, 46(8), 1651-1671.

132 Bakewell, L. L., Vasileiou, K., Long, K. S., Atkinson, M., Rice, H., Barreto, M., ... & Vines, J. (2018, April). Everything we do, everything we press: Data-driven remote performance management in a mobile workplace. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1-14),10.

133 Shin, H. C. (2019). The relationship between psychological contract breach and job insecurity or stress in employees engaged in the restaurant business. *Sustainability*, 11(20), 5709.

134 Manley, A., & Williams, S. (2022). 'We're not run on Numbers, We're People, We're Emotional People': Exploring the experiences and lived consequences of emerging technologies, organizational surveillance and control among elite professionals. *Organization*, 29(4), 692-713.

workers from already-marginalized communities.[135] Van Oort particularly emphasizes that such surveillance systems are accompanied by experiences of the emotional labour of surveillance whereby workers must constantly negotiate with both the surveillance technologies that control them and with the associated managerial perceptions of them as "suspect workers."

Overall, research overwhelmingly demonstrates that employee monitoring negatively impacts worker well-being. Studies consistently show that monitoring increases stress, anxiety, depression, and burnout, alongside physical ailments like headaches and sleep disturbances. These effects are exacerbated when monitoring feels intrusive, erodes employee perceptions of autonomy, and undermines trust in the workplace. Modern surveillance methods, which intensify scrutiny and can blur work-life boundaries, further contribute to worker insecurity, decreased self-esteem, and a heightened sense of pressure for those being monitored.

Employee productivity and general work performance

Workplace monitoring systems often have a detrimental effect on employee productivity and performance. Numerous studies demonstrate that monitoring can decrease work output, hinder effective problem-solving, and lower the overall quality of work. This negative impact stems from various factors, including increased stress, reduced autonomy, and how monitoring systems shift employee focus towards monitored tasks at the expense of other responsibilities. Additionally, the way monitoring is implemented, whether through supervisor, electronic, individual, or group-based methods, significantly influences its impact on performance outcomes.

Shin (2019) explored the effects of mystery shopping on service workers in South Korea, finding that the presence of mystery shoppers often caused workers stress, mainly due to the pressure of performing flawlessly to secure high evaluation scores. This stress was compounded by the subjective nature of the evaluations and the organizational demand to adhere to strict conduct rules, making it challenging for workers to meet sales targets and manage other customer needs effectively.[136] Similarly, Moore and Piece (2016) discussed the difficulties in integrating wearable self-tracking technologies in workplaces, particularly in knowledge-based settings, where such standard measures of productivity may not capture the varied performance routes, unlike in physical labour contexts like factories. These findings indicate that standardized performance metrics in office and administrative contexts may have an innate 'unevenness' that is not a meaningful reflection of actual performance. Charitsis (2019) critically assessed the impact of corporate wellness programs using Fitbit technology, noting that while data-driven corporate wellness programs are commonly viewed by employers as a means for improving employee health and productivity — and thus reducing corporate costs — the actual health benefits of self-tracking technologies remain empirically unsubstantiated.[137] The authors find that while

135 Van Oort, M. (2019). The emotional labor of surveillance: Digital control in fast fashion retail. *Critical Sociology,* 45(7-8), 1167-1179.

136 Shin, H. C. (2019). The relationship between psychological contract breach and job insecurity or stress in employees engaged in the restaurant business. *Sustainability*, 11(20), 5709.

137 Charitsis, V. (2019). Survival of the (data) fit: Self-surveillance, corporate wellness, and the platformization of healthcare. *Surveillance & Society*, 17(1/2), 139-144.

these programs are promoted to enhance health and productivity, they often do not deliver these benefits and may instead exacerbate anxiety, stigma, and health inequalities among employees.[138]

Gärtner and colleagues (2013) conducted a study to assess the impact of a workplace intervention used in healthcare settings that seeks to increase the help-seeking behavior, work functioning, and mental health of nurses and other healthcare professionals; the intervention involved screening employees for work functioning impairments and mental health complaints, and then inviting positively screened workers to see their occupational physician[139] Results of the study showed a significant improvement in work functioning among participants receiving the intervention compared to the control group, though no significant effects were observed regarding mental health complaints, suggesting that such monitoring programs may mitigate the impact of employee mental health concerns on workplace functioning (though they do not appear to address the core mental health concerns). Chang et al. (2015) found that employee trust in workplace monitoring policies positively influenced their commitment and compliance, whereas concerns about organizational overreach negatively affected trust and indirectly reduced commitment and compliance.[140] Tabak and Smith (2005) suggested that electronic monitoring could directly impact employee turnover and organizational commitment, depending on individual workplace experiences and their propensity to trust.[141]

Bernstrøm and Svare (2017) discovered that monitoring negatively affected intrinsic motivation due to perceived lack of trust, whereas a sense of control over workplace decisions boosted trust and motivation.[142] Weckert (2002) conducted a case study of change in supervisory monitoring policies for customer service agents at a large U.S. telecommunication call centre.[143] The study highlighted the benefits of involving employees in setting work standards after learning that changes to monitoring policies were viewed as unfair, which led to improved conditions and support for employee concerns. Pearson (1991) showed that participative monitoring schemes that provide extrinsic feedback could enhance worker motivation, satisfaction, and productivity, unlike situations where feedback was absent, which increased role ambiguity and decreased motivation and job satisfaction.[144]

138 Charitsis, V. (2019). Survival of the (data) fit: Self-surveillance, corporate wellness, and the platformization of healthcare. *Surveillance & Society*, 17(1/2), 139-144.

139 Gärtner, F. R., Nieuwenhuijsen, K., Ketelaar, S. M., van Dijk, F. J., & Sluiter, J. K. (2013). The mental vitality@ work study: effectiveness of a mental module for workers' health surveillance for nurses and allied health care professionals on their help-seeking behavior. *Journal of occupational and environmental medicine*, 55(10), 1219-1229.

140 Chang, S. E., Liu, A. Y., & Lin, S. (2015). Exploring privacy and trust for employee monitoring. *Industrial Management & Data Systems*, 115(1), 88-106.

141 Tabak, F., & Smith, W. P. (2005). Privacy and electronic monitoring in the workplace: A model of managerial cognition and relational trust development. *Employee Responsibilities and Rights Journal*, 17, 173-189.

142 Bernstrøm, V. H., & Svare, H. (2017). Significance of monitoring and control for employees' felt trust, motivation, and mastery.

143 Weckert, J. (2002). Trust, corruption, and surveillance in the electronic workplace. *Human choice and computers: issues of choice and quality of life in the information society*, 109-119.

144 Pearson, C. A. (1991). An assessment of extrinsic feedback on participation, role perceptions, motivation, and job satisfaction in a self-managed system for monitoring group achievement. *Human relations*, 44(5), 517-537.

Alder and Ambrose (2005) also observed that fairness in monitoring feedback improved participants' performance and satisfaction.[145] Martin, Wellen, and Grimmer (2016) surveyed a large sample of employed Australians to explore attitudes toward workplace surveillance, and whether these attitudes mediated the relationship between perceived levels of surveillance and counterproductive work behaviors (CWBs).[146] As anticipated, they found that higher levels of perceived surveillance correlated with more CWBs, and this association was mediated by attitudes towards surveillance. Interestingly, they also discovered that work empowerment mitigated the negative impact of unfavorable surveillance attitudes on CWBs, as employees with higher levels of empowerment did not exhibit adverse work behavior despite negative views on surveillance. In an experimental study, Aiello and Svec (1993) also found that both supervisor and electronic monitoring impaired task performance, but giving participants a sense of control or group monitoring mitigated the negative effects.[147]Chalykoff and Kochan (1989) used surveys[148] and Aiello and Kolb (1995) conducted a lab study[149] that further explored how monitoring affects job satisfaction, turnover propensity, and work performance, indicating varied impacts depending on the focus of monitoring and feedback. Snyder & Cornetto (2009) investigated workers' own perceptions of and experiences with workplace email monitoring through a survey involving 155 employees.[150] They found that participants exhibiting high levels of paranoia toward monitoring practices had low-quality workplace relationships with their coworkers and direct supervisors.

Griffith (1993) conducted an experiment to compare the effects of computer monitoring and supervisor monitoring on worker performance. In the study, forty-two women were assigned data entry tasks under three conditions: working alone, working under the direct supervision of a physically present supervisor, and working with computer monitoring but without the supervisor's physical presence. The results indicated that computer monitoring adversely affected work performance compared to working alone, whereas the physical presence of a supervisor actually improved performance.[151] Grant and Higgens (1989) conducted two studies focused on the impact of monitoring system design on employee attitudes and performance outcomes. These studies involved team-based work environments and included interviews with insurance claims processors and surveys of employees in various Canadian service firms. The findings suggested that the presence of monitoring systems did not automatically enhance or degrade productivity and performance. Instead, the effect of these systems depended significantly on their design and application. Specifically, the data collected by these systems influenced which tasks employees prioritized, often detrimentally affecting teamwork by encouraging individuals to focus on their own tasks at

145 Alder, G. S., & Ambrose, M. L. (2005). An examination of the effect of computerized performance monitoring feedback on monitoring fairness, performance, and satisfaction. *Organizational Behavior and Human Decision Processes,* 97(2), 161-177.

146 Martin, A. J., Wellen, J. M., & Grimmer, M. R. (2016). An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours. *The International Journal of Human Resource Management,* 27(21), 2635-2651.

147 Aiello, J. R., & Svec, C. M. (1993). Computer monitoring of work performance: Extending the social facilitation framework to electronic presence 1. *Journal of Applied Social Psychology,* 23(7), 537-548.

148 Chalykoff, J., & Kochan, T. A. (1989). Computer-aided monitoring: Its influence on employee job satisfaction and turnover. *Personnel Psychology,* 42(4), 807-834.

149 Aiello, J. R., & Kolb, K. J. (1995). Electronic performance monitoring: A risk factor for workplace stress.

150 Snyder, J. L., & Cornetto, K. M. (2009). Employee perceptions of e-mail monitoring from a boundary management perspective. *Communication Studies,* 60(5), 476-492.

151 Griffith, T. L. (1993). Monitoring and performance: A comparison of computer and supervisor monitoring 1. *Journal of applied social psychology,* 23(7), 549-572.

the expense of group goals. This focus on individual performance often left more complex customer service issues to other team members, fostering a perception of a hostile or stressful group environment.[152]

Larson and Callahan (1990) explored how performance monitoring affects productivity through an experiment with undergraduate students. They discovered that monitoring led to a significant increase in the amount of work completed, particularly when there were performance-related consequences. However, this monitoring caused employees to prioritize monitored tasks, neglecting those that were not monitored. The study cautioned that excessive monitoring might lead to perceived over-supervision, diminishing employee autonomy and motivation.[153] In a different laboratory experiment, Laird, Bailey, and Hester (2018) investigated the impact of different monitoring environments on problem-solving abilities. Participants were asked to solve puzzles under three conditions: no monitoring, human monitoring, and electronic monitoring. The results confirmed that intense monitoring environments negatively affected the participants' ability to find patterns and solve complex problems. However, for those with high confidence in their abilities, the adverse effects of monitoring were less pronounced or even reversed.[154] Brewer (1995) examined the effects of performance monitoring on task execution and effort allocation. In this study, individuals worked in groups on two tasks for 90 minutes while supervisors monitored either individual or group performance on one task. The results showed that monitoring individual performance caused participants to concentrate more on the monitored task, neglecting the unmonitored one. In contrast, when monitoring was applied to group performance, participants distributed their efforts more evenly across tasks, as the monitoring reduced the focus on individual performance comparisons by the supervisor. The implications of this study suggest that the method and focus of monitoring — in this instance, focusing on groups versus individuals — can profoundly influence employee behavior and the overall workplace environment.

Overall, these studies show that the way monitoring is implemented can have significant implications for employee productivity, motivation, and overall workplace dynamics. Monitoring that focuses on individual performance often results in increased stress, reduced autonomy, and a shift in focus towards tasks that are monitored at the expense of others. This not only detracts from overall productivity but can also foster a work environment characterized by distrust and reduced collaboration among team members. Conversely, monitoring that encompasses group performance tends to promote more balanced effort distribution and fosters a more cooperative and less stressful atmosphere. As such, the findings show that there are very good reasons for businesses to use monitoring that avoids highly individualized data collection that include, and even move beyond the risks to privacy workers' rights. Furthermore, co-design approaches to employee management can improve perceptions of fairness, mitigating the adverse psychological impacts of surveillance and enhancing employee satisfaction, trust, and potentially even productivity.

152 Grant, R., & Higgins, C. (1989). Monitoring service workers via computer: The effect on employees, productivity, and service. *National Productivity Review,* 8(2), 101-113.

153 Larson, J. R., & Callahan, C. (1990). Performance monitoring: How it affects work productivity. *Journal of Applied Psychology,* 75(5), 530.

154 Laird, B. K., Bailey, C. D., & Hester, K. (2018). The effects of monitoring environment on problem-solving performance. *The Journal of social psychology,* 158(2), 215-219.

Employee trust

Studies on the effects of electronic monitoring on trust in the workplace cover a range of topics, including its impact on management policies, the interplay between surveillance and employee autonomy, and the specific influence on how monitoring shapes organizational dynamics in the workplace.

Holland, Cooper, and Hecker (2015) conducted a detailed analysis using data from the 2012 Australian Electronic Workplace Survey involving 500 randomly selected employees. Their findings indicated a clear negative correlation between the extent of monitoring practices and trust in management. Employees subjected to increased monitoring were more likely to view management as deceptive and question their decision-making capabilities. The authors concluded that implementing more EMS practices can lead to decreased trust in management, potentially reducing employee engagement and organizational effectiveness.[155] Chang, Liu, and Lin (2015) similarly explored the dynamics of employee monitoring within the context of privacy boundaries by surveying full-time employees in organizations that practice monitoring. Their research highlighted that a control-oriented organizational culture amplifies perceptions of high monitoring levels, which stirs privacy concerns. These concerns, in turn, detrimentally affect trust in both the monitoring policies and the management implementing them. However, where trust in monitoring policies was established, there was a corresponding positive impact on employee commitment and compliance, illustrating the complex interplay between organizational culture, monitoring, and employee reactions.[156]

Whitener et al. (1998) shifted the focus to the role of managers in initiating trust, examining how organizational, relational, and individual factors influence managers' trustworthy behavior. Their framework suggests that trust is reciprocal, advocating that managers' proactive engagement in trustworthy behaviors can significantly foster employee trust, which in turn benefits organizational cohesion and effectiveness.[157] In a similar vein, Tabak and Smith (2005) researched the impact of monitoring on managerial cognition and relational trust development. They proposed that electronic monitoring provides cues to employees about the organizational culture, influencing their perceptions of fairness and trustworthiness of management. Their findings suggest that secretive monitoring practices are particularly damaging to trust, whereas transparency in monitoring practices helps maintain a positive perception among employees. They also noted that prior experiences and organizational culture influence managers' and employees' views on each other's trustworthiness, which then dictates the level and nature of monitoring.[158]

Weckert (2002) discussed the trade-offs between the need for workplace trust and the increasing prevalence of monitoring. He pointed out that while monitoring may enhance

155 Holland, P. J., Cooper, B., and Hecker, R. (2015). Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type. *Personnel Review,* 44(1), 161-175.

156 Chang, S. E., Liu, A. Y., and Lin, S. *(2015). Exploring privacy and trust for employee monitoring.* Industrial Management & Data Systems, 115(1), 88-106.

157 Whitener, E. M., Brodt, S. E., Korsgaard, M. A., and Werner, J. M. (1998). Managers as Initiators of Trust: An Exchange Relationship Framework for Understanding Managerial Trustworthy Behavior.

158 Tabak, F. and Smith, W.P. (2005) Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and Relational Trust Development. *Employee Responsibilities and Rights Journal*, 17, 173-189. https://doi.org/10.1007/s10672-005-6940-z

security and task-specific productivity, it often incurs significant costs in terms of reduced workplace trust, leading to minimal employee effort and high turnover rates. Weckert emphasized the delicate balance needed to maintain trust while implementing monitoring systems, concluding that "For a workplace to reach its full potential, trust is important" and that, while more "judicious" forms of workplace monitoring may not necessarily diminish workplace trust, it is always a risk and "once trust is lost, it is very difficult to regain".[159] Westin (1992) provided a case study from a Federal Express Corporation call center with similar findings that illustrate how changes in monitoring practices can significantly impact the traditional climate of trust between employees and employers. When monitoring was perceived as unfair, it led to employee resistance and protests, whereas a fair monitoring system, implemented within an environment of communication and mutual trust, was shown to support organizational productivity goals without harming employee relations.[160]

Berstrøm and Svare (2017) found in their study of 3,015 Norwegian employees that monitoring inversely affected employees' feelings of trust. Conversely, giving employees control over workplace decisions was positively related to higher felt trust, which in turn enhanced their intrinsic motivation and sense of mastery over their work.[161] Jensen and Raver (2012) also focused on the interplay between employee control over their work and supervisory surveillance. Their empirical studies showed that while self-management promoted positive organizational behaviors and trust, the addition of surveillance undermined these benefits, leading to increased counterproductive work behaviors.[162]

In two meta-analytic studies on the topic, Backhaus (2019) and Kalischko and Riedl (2021) provided broader overviews. Backhaus included 85 studies that focused on the impact of electronic monitoring on various outcome variables in the workplace, including employee performance, psychological stress, work motivation, satisfaction, behavior, organizational trust, and perceived control. The findings indicated adverse effects of monitoring on perceived stress, mental demand, job motivation, satisfaction, organizational trust, and perceived control.[163] Kalischko and Riedl's (2021) review of electronic performance monitoring (EPM) literature highlights mixed empirical findings regarding the impact of EPM on employee trust. Their review emphasized the importance of trust in the workplace and led them to conclude that the majority of EPM studies show monitoring negatively impacts workplace trust.[164]

The findings across these studies consistently show that increased monitoring can undermine trust in management, decrease employee engagement, and adversely alter the dynamics of the work environment. When monitoring practices are perceived (and experienced) as intrusive or unfair initiatives that diminish privacy and erode trust, alienation

159 Weckert, J. (2002). Trust, corruption, and surveillance in the electronic workplace. Human choice and computers: issues of choice and quality of life in the information society, 109-119.

160 Westin, A. F. (1992). Two key factors that belong in a macroergonomic analysis of electronic monitoring: Employee perceptions of fairness and the climate of organizational trust or distrust. *Applied Ergonomics,* 23(1), 35-42.

161 Bernstrøm, V. H., & Svare, H. (2017). Significance of monitoring and control for employees' felt trust, motivation, and mastery.

162 Jensen, J. M., & Raver, J. L. (2012). When self-management and surveillance collide: Consequences for employees' organizational citizenship and counterproductive work behaviors. *Group & Organization Management,* 37(3), 308-346.

163 Backhaus, N. (2019, January). Context sensitive technologies and electronic employee monitoring: a meta-analytic review. In *2019 IEEE/SICE international symposium on system integration (SII)* (pp. 548-553). IEEE.

164 Kalischko, T., & Riedl, R. (2021). Electronic performance monitoring in the digital workplace: conceptualization, review of effects and moderators, and future research opportunities. *Frontiers in psychology,* 12, 633031.

in workplace activities ensues. The research also points out, however, that transparency in monitoring practices and giving employees control over their work conditions can mitigate some of these adverse effects. Studies also highlight the reciprocal nature of trust, emphasizing the importance of management's role in fostering a trusting environment through transparent and fair practices.

Section IV: The datafication of work, surveillance trends, and privacy implications

The datafication of organizations and increased employee visibility

Through ongoing technologization and datafication a broad range of organizational processes become increasingly visible with the possibility of monitoring and forms of automated management becoming continuous, passive, and more comprehensive. Consequently, data collection expands the scope of employee visibility for managers and organizations, encompassing both work and private activities. This trend raises two key concerns:

1. **Non-purposeful or incidental data collection:** The collection of personal information extending beyond workplace activities, as it is often "incidental" to legitimate business operations. This may include excessive monitoring that intrudes into private life (beyond work activities), as well as the turn towards acquiring information from employment data brokers, such as Claro.[165]
2. **Predictive analytics and inferred insights:** The scale and intensity of data collection raise concerns about its integration into machine learning analysis, potentially revealing intimate, non-work-specific information about employees' personal lives, health, preferences, and behaviors, even when the initial data appears related to legitimate business activities.[166]

Drawing on insights from Solove (2024),[167] these developments pose serious challenges to the existing privacy regulatory paradigm that relies on definitions of personal information to manage surveillance-related harms. When incidental or non-personal information can be used to derive insights or conclusions about a person's private life, regulation through categories of information is unfit for purpose.

Automated / algorithmic management

Another major trend is toward the consistent integration of predictive analytics, machine learning, and 'automated management' into business organization operations. While algorithmic management is most synonymous with 'on-demand' platform work, its

165 Claro refers to itself as a global labour intelligence platform that can facilitate searches on "all workforce-related information on the public internet." See https://www.claroanalytics.com/platform.

166 See for instance Knight, W. (2023, October 17). AI Chatbots Can Guess Your Personal Information From What You Type. *Wired*. https://www.wired.com/story/ai-chatbots-can-guess-your-personal-information/

167 Solove, D. J. (2024). Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data. *Northwestern University Law Review*, 118(4), 1081-1138.

permeation into a broad range of sectors carries significant impacts, including a vast range of employment decisions relating to the management of employee work tasks, hiring, promotion, termination, disciplinary decisions, and many more.

The permeation of algorithmic decision making into a broad swathe of employment decisions raises fundamental questions about worker privacy (particularly the scope of data sets that may include information that extends beyond the work environment (both spatially and temporally). It also raises serious concerns about what rights workers have about decisions that are made about them in the workplace, and whether they have a right to transparency, explainability, and accuracy without fear of retaliation. These elements are covered in further detail in the legal section.

The ongoing sensorization of the workplace through IoT and wearable technologies

The continued sensorization of the workplace through IoT and wearable technologies is an ongoing trend that significantly impacts how workplaces are managed and how employees interact with their environments (both at work and privately). In sectors like manufacturing, construction, and mining, wearables can potentially improve health and safety outcomes by tracking vital signs or detecting hazardous conditions thereby triggering alerts that can prevent harmful exposures or accidents. However, continuous monitoring, or monitoring that exceeds this narrow purpose of health, (including biometrics or other private sensitive information) introduces serious risks for employee autonomy and workers' rights. Careful attention is needed throughout the technology development and regulation lifecycle. This includes design that adheres to privacy principles (such as data minimization) and contextual integrity norms, as well as laws and regulations that ensure safety gains don't establish conditions that pave the way for broader violations of workers' rights.

Remote monitoring technologies / employee monitoring applications

Another significant trend in workplace surveillance and employee monitoring is the growing use of Employee Monitoring Applications (EMAs). The rise of remote work, catalyzed and accelerated through the COVID-19 pandemic, has prompted employers to turn to surveillance-related solutions to shore up concerns about loss of productivity or even threats to cybersecurity. EMAs present some of the most intensive forms of monitoring that can exist in the workplace, often gathering a broad range of sensitive data types while in the process of being used for "legitimate" business purposes. Research from Thompson and Molnar (2023) has shown that while managers are increasingly turning towards the use of EMAs,[168] as the section of this report on the adverse impacts of employee monitoring indicates, they contribute to a broad range of corrosive impacts.[169] Urgent clarity is needed on the strict use or prohibition of EMAs to avoid the prospect of regulating EMA-related harms into existence.

168 Thompson, D. and Molnar, A. 2023. Workplace Surveillance in Canada: a survey on the adoption and use of employee monitoring applications. *Canadian Review of Sociology*, 60(4): 801-819.

169 See also Ravid, D. M., Tomczak, D. L., White, J. C., & Behrend, T. S. (2020). EPM 20/20: A review, framework, and research agenda for electronic performance monitoring. *Journal of Management*, 46(1), 100-126

Section V: The legal environment

Workplace monitoring and algorithmic management, with their diverse forms and impacts, are addressed by a fragmented legal environment. Relevant legal frameworks range from those specifically focused on electronic monitoring and surveillance to broader areas like privacy and data protection, employment law, collective agreements/contracts, labour law (including arbitration), civil law (tort, contract), criminal law, and constitutional human rights law.

A comprehensive analysis of this regulatory landscape across all jurisdictions falls beyond the scope of this report. Instead, this section of the report focuses on laws and regulations directly safeguarding employee privacy, data protection, and human rights in the workplace. This comparative legal review will examine models and legislative proposals that could contribute to future robust models that protect workers' rights in the workplace.

Before undertaking this analysis, however, it is crucial to recognize that a common privacy metric — the notice and consent model — alone cannot adequately determine the practical adequacy of workplace privacy and employee data protection.[170] The inherent power differential between employers and employees, coupled with the employee's reliance on their income, undermines the notion of freely given consent.[171] Employees may feel pressured to agree to monitoring, fearing repercussions if they refuse. Furthermore, while notification is an important aspect of making workplace monitoring practices more transparent, on its own is an insufficient mechanism for upholding meaningful privacy protections. Therefore, relying solely on a notice and/or consent regime as a basis for employee monitoring remains a controversial approach. Some jurisdictions, as discussed below, explicitly restrict, or reject, the use of consent in most employee monitoring scenarios.[172]

Canada

Individuals in Canada have a right to privacy at work regardless of whether they are located on premises, are hybrid or remote working, or whether they are using an employer-issued or personal device. Privacy legislation that relates to employee monitoring and privacy in Canada stretches across a range of federal and provincial jurisdictions.

Privacy Act

The *Privacy Act* is a federal law governing how the Government of Canada collects and handles personal information. While the act does not specifically target employee privacy, its provisions do extend to federal public sector employees. Under the *Privacy Act*, federal government employers may only collect employee information directly related to a government program or activity. This information must be used for its original collection purpose or one consistent with that purpose. However, an employer may use employee

170 European Parliament, "Article 28, Working Party Guidelines on consent under Regulation 2016/679." April 10, 2018. https://ec.europa.eu/newsroom/article29/items/623051

171 Nguyen, A. (2021). The constant boss: Work under digital surveillance. Data & Society Report. 19 May. https://apo.org.au/node/312352

172 European Parliament, "Article 28, Working Party Guidelines on consent under Regulation 2016/679." April 10, 2018. https://ec.europa.eu/newsroom/article29/items/623051

personal information for a different purpose with employee consent or if a specific exemption under section 8(2) of the act applies. For example, a federal government employer using CCTV for security purposes cannot, without employee consent, repurpose the video for performance management unless a section 8(2) exemption applies. Section 8(2) exemptions include requirements that employees must generally be informed about the reasons for collecting their information at the time of collection, with exceptions on disclosure included for law enforcement and legal proceedings.[173] [174]

Personal Information Protection and Electronic Documents Act

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is the primary piece of legislation with broad reach across Canada that regulates consumer data handled by the private sector. However, PIPEDA also applies to federally regulated employee information, meaning information about workers employed in federal works, undertakings, and businesses (FWUBs), such as banks, airlines, inter-provincial transportation, and telecommunications companies.[175] [176]

Employees protected by PIPEDA are provided certain limited rights regarding their personal information. Specifically, employer monitoring under PIPEDA must generally clearly notify and outline reasons for collecting employee data, must obtain consent, must collect only for purposes that a reasonable person would consider appropriate, and must limit collection to these purposes.[177] Employers must also maintain accurate information, and in return, employees have the right to access personal information held by their employer and can challenge any perceived inaccuracies.[178]

However, several exceptions exist under PIPEDA that shape how employers can collect, use, and disclose personal information. An exception to consent "to establish, manage or terminate" an employment relationship under PIPEDA exists, even if other requirements in the Act still apply, such as accountability, notification (informing the employee), and limits on collection, use, disclosure, and retention of personal information.[179] Importantly, legal requirements governing the handling of personal information cannot be waived by an individual's consent. Furthermore, collection and disclosure can occur without notification or consent in legal cases relating to national security, investigations into a breach of Canadian/foreign law, court orders.[180]

In *Eastmond v Canadian Pacific Railway,*[181] the Federal Court upheld employee privacy rights by limiting the repurposing of workplace video surveillance, originally installed for security reasons, toward productivity monitoring. While this ruling does not exclude

173 S.8(2) is extensive and covers a range of activities https://laws-lois.justice.gc.ca/eng/acts/p-21/section-8.html

174 The leading case relating to employee privacy under the *Privacy Act* is Dagg v. Canada (Minister of Finance), [1997] 2 S.C.R. 403.

175 PIPEDA, section 4(1)(b).

176 Office of the Privacy Commissioner of Canada. (2023, May 29). Privacy in the Workplace. https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/02_05_d_17/

177 PIPEDA, section 5(1).

178 PIPEDA, section 4(9).

179 PIPEDA, section 7(3)(a)

180 PIPEDA, section 7(3)(d.1) and 7(3)(d.2)

181 *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 (CanLII). https://canlii.ca/t/1hclc; Monkhouse, H. (2020, January 15). Privacy in the workplace: Bosses who spy on you. https://canliiconnects.org/en/commentaries/70081

'productivity' as a legitimate purpose for workplace monitoring, it underscores that employers must provide a clear justification for each specific use of workplace surveillance technologies.

A small handful of relevant PIPEDA cases have been released over the years that lend further detail to the practical application of the Act as an employee privacy law. Specifically, they reaffirm that personal information shall not be used or disclosed for purposes other than those for which it was collected (unless with consent or as required by law)[182] and that employers cannot use surveillance for a purpose that was "not likely to be considered appropriate" when considering the reasonableness test (in this instance, whether the camera was demonstrably necessary to meet a specific need, whether the monitoring is likely to be effective in meeting that need, whether the loss of privacy is proportional to the benefit gained, and whether there is a less privacy-invasive way of achieving the same end).[183] Another important case on an internet service provider installing web cameras to monitor the performance of employees lends important insight into the limits of productivity monitoring under PIPEDA. This case involved an ex-employee registering a complaint that managers' focusing non-recordable, but remotely real-time viewable, cameras on sales, marketing, and technical support staff was excessive under PIPEDA.[184] The assistant commissioner agreed, citing that a much less-intrusive method of addressing security and worker productivity already existed, that continuous surveillance was deemed, more in place as a strategy of deterrence, and that doing so imposed negative impacts on worker autonomy.[185]

Overall, the *Privacy Act* and PIPEDA function indirectly for a narrow cross section of workers in Canada. Most employees fall under provincial authority and are only subject to provincial information protection legislation where it exists — and each offer a different approach when compared to PIPEDA.

The following sections focus on provincial privacy legislation in British Columbia and Alberta, before moving on to the unique jurisdiction and legal environment of Quebec civil law. The provincial section concludes with an overview of Ontario.

British Columbia and Alberta

Alberta and British Columbia's laws — the *Personal Information Protection Acts* (PIPAs), as well as the respect *Freedom of Information and Protection of Privacy Acts* (FIPPAs)—are very similar in how they approach personal information in the workplace. Each provincial statute permits employers to collect, use, and disclose employee personal information without consent if the purpose is connected to reasonable purposes related to recruiting, managing, or terminating personnel, or for other legal reasons, such as through a lawful access request. The PIPAs also require reasonable security measures to protect employee data against unauthorized access.

182 PIPEDA Case Summary #264 - Video cameras and swipe cards in the workplace. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2004/pipeda-2004-264/

183 PIPEDA Case Summary #290 - Video surveillance cameras at food processing plant questioned. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2005/pipeda-2005-290/

184 PIPEDA Case Summary #279 - Surveillance of employees at work. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2004/pipeda-2004-279/

185 PIPEDA Case Summary #279 - Surveillance of employees at work. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2004/pipeda-2004-279/

Like PIPEDA, where there is an exemption to consent requirements for managing the employment relationship, Alberta's and B.C.'s PIPAs waive the consent requirement. However, unlike PIPEDA, these acts have additional requirements in place such as notification that are not present in PIPEDA. For instance, in B.C. and Alberta, employers do not need to ask for consent, but must notify employees what is being monitored, provide reasons for monitoring (that must be "necessary for a reasonable purpose"), and include how employee personal information will be used.

The practical adequacy of these notices is largely unclear when it comes to how and whether employees are meaningfully informed. When understanding the practical adequacy of these provisions, the laws seem to indicate that given organizations should only collect personal information that is necessary for a reasonable purpose, excessive surveillance that intrudes into private lives could be problematic. Regarding the practical adequacy of notification, while organizations are obligated to notify their employees, it is unclear how specific these notices are in practice such that they may not amount to a meaningfully informed communication about monitoring and data handling practices.

In 2015, the Office of the Information and Privacy Commissioner for British Columbia (B.C. OIPC) published an investigation relating to FIPPA that focused on how a public sector workplace was using monitoring software that collected employee information acquired through screenshots, keystroke logging, and online tracking activity including website visits and messaging. The public body insisted that the spyware was to facilitate IT security, however, the B.C. OIPC found that the collection of personal information in "keystroke logs and screenshots, program activity, email, and user logon information"[186] amounted to an excessive unauthorized collection of employee personal information that went beyond what is "directly related to and necessary for the protection of IT systems and infrastructure".[187] Two years later, the B.C. OIPC published a guidance document further detailing how workplace monitoring technologies such as CCTV, employee monitoring software, and GPS tracking can be interpreted under FIPPA and PIPA.

Quebec

Quebec has patchwork legislation to protect employee privacy. This patchwork stems from *An Act Respecting the Protection of Personal Information in the Private Sector* (in place since 1993), which is read in conjunction with the *Quebec Charter of Human Rights and Freedoms*, and the *Quebec Civil Code*.

Though the *Act Respecting the Protection of Personal Information in the Private Sector* does not directly address workplace monitoring, it also does not exempt employee information held by employers. Notably, the act was amended in 2021 by the enactment of Bill 64 *An Act to modernize legislative provisions as regards the protection of personal information*.[188] This amendment introduced a variety of changes that came into force in three stages: September 2022, September 2023, and September 2024. These changes expanded the

186 Investigation Report F15-01 – Information & Privacy Commissioner for British Columbia, p.27. https://www.oipc.bc.ca/documents/investigation-reports/1688

187 Office of the Information and Privacy Commissioner for British Columbia. (2017 November). EmployeeMPLOYEE Privacy Rights, p. 4 https://www.oipc.bc.ca/guidance-documents/2098, p. 4

188 An act to modernize legislative provisions as regards the protection of personal information, SQ 2021, c 25.

investigative powers of the Commission d'accès à l'information (the Commission on Access to Information) and increased the maximum amount of administrative monetary penalties to the greater of $10 million or two per cent of the enterprise's worldwide turnover in the previous year. It also placed new consent requirements for enterprises collecting, using, or disclosing personal information, placed limits on how personal information can be handled, and created a requirement for organizations to conduct privacy impact assessments. Relating specifically to employment, organizations cannot refuse an individual's request for employment based on that individual's refusal to disclose personal information, except when: collection is necessary for contractual reasons, collection is authorized by law, or there are reasonable grounds to believe that the request is not unlawful.[189] While this may offer some protection against excessive collection, it seems likely that employers would still be able to justify a considerable amount of information collection from prospective employees. There is also a provision of the act forbidding reprisals against individual who file complaints with the Commission on Access to Information, and the act specifies that "the demotion, suspension, dismissal or transfer of a person or any other disciplinary measure or measure that adversely affects a person's employment or conditions of employment is presumed to be a reprisal."[190] This article provides some support to employees seeking to enforce their rights under this act, although truly preventing reprisals in the workplace may be difficult given the power dynamics of the employment relationship.

The Quebec Charter, notable for its application to the private sector, offers workers (not only employees) the right to "fair and reasonable conditions of employment" and recognizes workers' "health, safety and physical well-being."[191] Given the research on impacts of employee monitoring above, it is conceivable that some invasive forms of privacy in the workplace may be considered a violation of this Charter right. The Charter also goes further, however, to include protections of privacy and dignity that apply to all individuals, including workers.

The Quebec Charter, with its preamble emphasizing "respect for the dignity of the human being,"[192] sets the core foundation of all Quebec legislation and private sector policies. It explicitly guarantees that "Every person has a right to the safeguard of his dignity, honour, and reputation,"[193] and that "Every person has a right to respect for his private life."[194] Quebec's Civil Code further reinforces the workers' dignity and right to private life by explicitly obligating employers to "take any measures consistent with the nature of the work to protect the health, safety and dignity of the employee" as part of the employment relationship.[195] While these aspects project a respect for dignity, as Avner Levin notes, exemptions for government agencies to disclose personal information without consent if required to exercise their duties could pose a contradiction to the emphasis on dignity.[196]

189 An act to modernize legislative provisions as regards the protection of personal information, SQ 2021, c 25.

190 Act respecting the protection of personal information in the private sector, CQLR c P-39.1, art 81.2.

191 Quebec Charter, supra note 29, s. 46. https://www.legisquebec.gouv.qc.ca/en/document/cs/c-12

192 Quebec Charter, preamble. https://www.legisquebec.gouv.qc.ca/en/document/cs/c-12

193 Quebec Charter, s. 4 https://www.legisquebec.gouv.qc.ca/en/document/cs/c-12

194 Quebec Charter, s. 5. https://www.legisquebec.gouv.qc.ca/en/document/cs/c-12

195 Quebec Civil Code, R.S.Q. 1991, c. 64, art. 2087

196 Levin, A. (2007). Big and little brother: The potential erosion of workplace privacy in Canada. *Canadian Journal of Law and Society/La Revue Canadienne Droit et Société*, 22(2), 197-230.

Ontario

Ontario is another jurisdiction with an uneven and fragmented patchwork of muted workplace privacy legislation. For Ontario's 1.6 million public sector workers, the *Freedom of Information and Protection of Privacy Act* (FIPPA) governs the collection, use, disclosure, retention, security, and disposal of employee personal information by employers. FIPPA is, however, severely limited as it relates to employee privacy rights. Amendments in 1995 to FIPPA removed access to labour relations and employment-related records from the scope of the act, which severed the connection to privacy rules governing these records. In 2002, for example, the Ontario IPC concluded that because of these amendments, it had no jurisdiction over two privacy complaints, the first regarding video surveillance on a picket line[197] and the second concerning the use and disclosure of an employee's personal information in a union-management meeting involving disciplinary matters.[198] Ultimately, Ontario's FIPPA, even when it first came into force in 1987, has been described as "fundamentally deficient" as it relates to the practical adequacy of the Office of the Information and Privacy Commissioner of Ontario to facilitate compliance with rules governing the collection, use, and disclosure of employee personal information.[199] Since then, a series of judicial and legislative changes have even further undermined any semblance of privacy rights, including for employees.[200]

It is only in recent years that the provincial government has made an attempt to address employee privacy in the private sector. Ontario's Bill 88 to enact the *Working for Workers Act*, has a stated aim to increase transparency and protect worker privacy in Ontario. It requires companies with 25 or more employees (including full-time, part-time, casual, and assignment workers) to provide a written policy disclosing electronic monitoring practices.[201] This policy must outline how monitoring occurs, the circumstances in which it is used, and the purposes for data collection. Employers must provide this policy to employees within 30 days of its creation or their hiring date and retain it for three years after it is no longer active. Workers have the right to file a complaint with the Minister of Labour, Training and Skills Development if they do not receive the policy. Further, Ontario's Bill 149 to enact the *Working for Workers Four Act*, stipulates that any employer who publicly advertises a job must include a disclosure in the job posting if they plan to use "artificial intelligence to screen, assess, or select applicants for the position."[202] However, the *Working for Workers Act* primarily focuses on notification and transparency, not restricting any practices of monitoring, algorithmic management, or data handling itself. As a result, Thompson and Molnar (2023) deem it "ineffective" and "incomplete" when it comes to providing meaningful privacy protections for Ontario workers, arguing for more specific provisions to meaningfully address the broader panoply of workplace surveillance harms.[203]

197 Privacy Complaint Report PC-020022-1 (Ministry of Public Safety and Security).

198 Privacy Complaint Report PC-020052-1 (Ministry of Public Safety and Security).

199 Berzins, C. (2014). Ontario's Freedom of Information and Protection of Privacy Act after 25 Years: A Critical Assessment. Advoc. Q., 43, 80.

200 Berzins, C. (2014). Ontario's Freedom of Information and Protection of Privacy Act after 25 Years: A Critical Assessment. Advoc. Q., 43, 80.

201 *Working for Workers Act*, c 7, Part XI.1.

202 *Working for Workers Four Ac*t, 3, 8.4.

203 Thompson, D. and Molnar, A. 2023. Workplace Surveillance in Canada: a survey on the adoption and use of employee monitoring applications. *Canadian Review of Sociology*, 60(4): 801-819.

Proposed federal Bill C-27

Against this backdrop of 'ambivalent' privacy protections for workers in Canada[204], the Federal government is currently proposing Bill C-27, a raft of new legislation relating to privacy and algorithmic management. The following section analyzes the *Artificial Intelligence and Data Act* (AIDA) as well as the *Consumer Privacy Protection Act* (CPPA) as they relate to electronic monitoring and the use of algorithms in the work environment.

Artificial Intelligence and Data Act

The *Artificial Intelligence and Data Act* (AIDA) applies to a range of 'high impact' algorithmic management technologies, such as employment screening systems and biometric systems. Employers that use 'high impact' algorithmic management technologies — such as employment screening algorithms, biometric systems, or EMAs that rely on algorithmic scoring — are subject to a range of requirements.

Employers responsible for the operation of a high-impact algorithmic system under AIDA are also required to conduct ongoing monitoring and risk mitigation measures. Specifically, they must conduct evaluations to detect potential biases or discrimination in AI-systems, to monitor and document these risks through audits, and to identify risk mitigation strategies.[205]

Notification obligations require that employers publish a plain language description of the system on a publicly available website that details: (a) how the system is used; (b) the types of content it generates and the decisions, recommendations or predictions that it makes; (c) the mitigation measures that have been established in relation to the identification of risks; and (d) any other information that may be prescribed by regulation.[206] Employers are obligated to maintain records to fulfill compliance with the proposed act.[207]

Ministerial powers under AIDA would allow for ministerial order of an audit[208] to evaluate contraventions of the act that result in material harm[209] or where an organization fails to establish measures that meet data anonymization requirements.[210] Any public interest disclosures resulting from the audit are subject to confidentiality obligations, for instance, the Minister would not be permitted to publish "confidential business information." The tension between these competing values as they relate to practical outcomes is worthy of further inquiry. The proposed act also introduces the potential for administrative monetary penalties (AMPs) to promote compliance that would be administered by the creation of an Artificial Intelligence and Data Commissioner. [211]

---

204 I use the term ambivalent here to describe how the existing legislative environment in Canada is almost uniformly premised on outdated legislation that is not 'fit for purpose' as legislation that would explicitly address the specific concerns of employee privacy in the contemporary digital workplace.

205 AIDA, s. 9

206 AIDA, s. 11(1)(a-d)

207 AIDA, s.10

208 AIDA, s.13, 14, and 15

209 AIDA, s.12

210 AIDA, s.6

211 AIDA, s.29; Also, the amounts of penalties are noted at s.30(3), as well as General Offences noted in s.38-40.

Consumer Privacy Protection Act

The *Consumer Privacy Protection Act* (CPPA), another key element of Bill C-27, aims to update the regulatory framework governing the collection, use, and disclosure of personal information in commercial activities, which affects both business-consumer and employer-employee relationships in federal works, undertakings, and businesses (FWUBs). The CPPA replicates some aspects, but also introduces other notable changes relating to employee privacy from its predecessor, PIPEDA, in several key areas.[212]

There are two main provisions that relate to the employment relationship in the CPPA. Section 23 states that "an organization may collect, use or disclose an individual's personal information without their knowledge or consent if it was produced by the individual in the course of their employment, business or profession and the collection, use or disclosure is consistent with the purposes for which the information was produced."[213] Referring more explicitly to FWUBs, section 24 states that an organization that operates a FWUB "may collect, use or disclose an individual's personal information without their consent."[214] The collection and handling of FWUB-employee specific data without consent, however, can only occur if employees are notified (absent any specifics about how this notification must occur beyond including purposes)[215] and if, like PIPEDA, the collection, use, and disclosure is "necessary to establish, manage or terminate an employment relationship between the organization and the individual."[216]

The implied consent model operates in tandem with a notification regime. Employers are required to publish a plain language notification that explains the organization's policies and practices under the CPPA. Specifically, they are required to include the following information: a description of the type of information under the organization's control, a general account of how the organization uses the information and how it applies the exception of the requirement to obtain consent, a general account of the organizations' use of any automated decision system "to make predictions, recommendations, or decisions about individuals that could have significant impact on them," whether or not the organization carries out any international or interprovincial transfer or disclosure of personal information that "may have reasonably foreseeable privacy implications," information about retention periods that apply to sensitive personal information, how individuals can make requests for disposal of their personal information, and the business contact information of an individual to whom complaints or requests for information can be made.[217]

Other provisions of the CPPA also relate to the employment relationship, specifically, to data retention and disposal schedules, workers' rights regarding accuracy and access, and security safeguards. Regarding data retention and disposal, employers are prohibited from retaining employee information longer than necessary to fulfil the purposes for which the

212 CPPA, s.6(1)(b)
213 CPPA, s.23
214 CPPA, s.24
215 CPPA, s.24(b)
216 CPPA, s.24(a)
217 CPPA, s.62(1)(2)(a-g)

information was collected or to comply with the CPPA itself.[218] Employers are required to take into consideration the sensitivity of the information that has been collected.[219]

Regarding the accuracy and access of personal information, employers are obligated to take reasonable efforts to ensure that the personal information they hold is accurate, up-to-date, and complete,[220] this requirement is particularly important given they are using the information to make decisions about employees.[221] Employees are also afforded access rights. For instance, they may request what information is held about them, how this information is used, and whether it has been disclosed (and who it may have been disclosed to).[222] Access requests also apply for workers to receive explanations regarding uses of automated decision systems, if the system has been used "to make a prediction, recommendation or decision about the individual that could have a significant impact on them."[223]

And lastly, regarding security safeguards, employees are afforded a certain degree of protection. Employers are required to "protect personal information through physical, organizational, and technological security safeguards," and the level of the protection provided "must be proportionate to the sensitivity of the information".[224] Employers must consider factors such as the quantity, distribution, format, and method of storage of the information,[225] to ensure it is protected against "loss, theft, unauthorized access, disclosure, copying, use and modification."[226] If any data breach occurs, employers are required to consider whether it is reasonable under the circumstances that a real risk of significant harm could arise to an individual.[227] If it does, they are required to report to the commissioner as well as to notify impacted individuals as soon as is feasible.[228] As is typical, these requests are subject to rules surrounding response times, costs, and reasons for refusal.

The CPPA may indirectly apply to the use of contemporary electronic monitoring technologies (such as EMAs) in a couple of instances. For example, if EMAs engage in data collection that exceeds the originally stated purpose of managing employment relationships (e.g., monitoring intimate behaviors, emotional states, or personality), this could become a concern under the CPPA. Similarly, outsourcing data to third parties might trigger data processing and transfer requirements, especially if these third parties handle employee personal information across borders. Additionally, the CPPA's data breach notification requirements and penalties would certainly apply to any EMA-related data breach.

218 CPPA, s.53(1)(a)(b)
219 CPPA, s.53(2)
220 CPPA, s.56(1)
221 CPPA, s.56(2)(a)
222 CPPA, s.63(1)
223 CPPA, s.63(3)(4)
224 CPPA, s.57(1)
225 CPPA, s.57(2)
226 CPPA, s.57(3)
227 CPPA, s.58(1)
228 CPAA, s.58(2-6)

Summarizing Canada's patchwork employee privacy landscape

Canada's current patchwork of federal and provincial privacy laws offers a complex landscape when it comes to regulating workplace monitoring and addressing potential harms. Approaches are inconsistent between provinces, the federal level, and across public and private sectors, leading to confusion and, ultimately, ongoing vulnerability for many workers.

A common theme across laws in B.C. and Alberta, as well as the proposed CPPA is their focus on notification and consent (including its waiver). Ontario, however, only recently introduced notification, historically ignoring consent (and employee privacy protections) entirely. While the 'free and informed' consent model is unsuitable for the workplace power imbalance, these laws lean heavily on notification. Though deeper research is needed to fully evaluate the practical adequacy of these notices, their current form (without any conditions on their specificity) is likely insufficient. Crucially, overreliance on notification should not substitute for comprehensive privacy protections nor diminish an employee's reasonable expectation of workplace privacy. This is particularly concerning in jurisdictions like BC and Alberta, where "reasonableness" is often determined from the employer's perspective, not the employees. However, while Quebec's civil law approach, and in particular its emphasis on dignity as a mediating value for employee rights presents some positive affirmation for workers' rights, it is not likely that this emphasis can be straightforwardly introduced into common law provinces given the lack of overarching framework structuring worker privacy rights.

As mentioned, most laws currently in existence tend to prioritize the employers' business need to collect data, and sometimes in a way that is deemed reasonable by management themselves. This is done in such a way that it tends to overlook the underlying power dynamic between employers and employees — in ways that avoid any robust justification as to how (or what the research says about how) intrusions might impact that need. Ontario, like the other provinces, similarly, mandates employer notice, but it doesn't provide workers with sufficient control or autonomy over monitoring. Ontario has particularly limited regulations governing workplace surveillance practices, standing out as being particularly weak, having only notification but no other protections for workers that relate to access, accuracy, purpose limitations, employer-centric reasonableness, or whistleblower protections, among other measures.

Similarly, modern technologies and the trend toward algorithmic management expresses a fuzzy relationship with the scope of existing law. B.C., Alberta, and Ontario laws have no direct connection to the harms that can emerge from modern workplace monitoring and management practices. While AIDA makes an early attempt at introducing workers' rights to transparency and explainability, it is limited in detail and beset by a notable conflict in its governance structure where the Minister for Innovation, Science, and Economic Development Canada is both responsible for administration of harms as well as furthering innovation.[229]

229 For a detailed analysis of additional concerns regarding AIDA, see Clement. A. 2023. No AIDA is better than this AIDA. A brief submitted to The Standing Committee on Industry and Technology (INDU) on Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, accessed at: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12743452/br-external/ClementAndrew-e.pdf

Overall, Canada's patchwork of privacy laws inadequately addresses the potential harms of workplace monitoring. Provincial legislation, in particular, could benefit from clearer articulation of worker rights and limitations on employer monitoring practices, including algorithmic management.

United States

Federal

At the federal level, the *Electronic Communications Privacy Act* (ECPA) — Title I the *Wiretap Act*, and Title II the *Stored Communications Act* (SCA), provide no meaningful employee privacy protection, and have been referred to as affording "limitless" opportunity for employer surveillance.[230] Title I, the *Wiretap Act*, allows for one-party consent monitoring (among other concerns). And Title II, the SCA, prohibits access to stored information without authorization (which can be sanctioned through contract), a condition that is only relevant to the employer-employee relationship if such access occurs outside of work hours.[231]

The *Computer Fraud and Abuse Act* (CFFA) — a U.S. federal law that prohibits unauthorized access to computers and computer systems, exceeding authorized access, and obtaining information protected under the law — similarly overlooks the current characteristics of the modern workplace. In common instances where employers own and provide business devices to employees, or where employees consent to installing monitoring software on their own device, the CFAA would not address these forms of authorized access.[232]

Given these outdated and inapplicable frameworks, lawmakers have recently proposed new federal legislation to regulate workplace surveillance technologies.[233] Cited as the *Stop Spying Bosses Act*, the bill attempts to "prohibit, or require disclosure of, the surveillance, monitoring, and collection of certain worker data by employers, and for other purposes."[234]

Notification, transparency, data access, and correction

Specifically, the bill would require that employers disclose what workplace surveillance is being undertaken including what, where, when, how, and how often (frequency) data are being collected, the business purposes for which the data are being used, the identity of any third party supplier being used that may implicate data transfers or commercial purchases and acquisitions, and "how such workplace surveillance affects employment-related decisions by the employer, including with regard to the assessment of the performance and productivity of the covered individual."[235] These conditions are notably more detailed than in Ontario's *Working for Workers Act*.

---

230 Ajunwa, I., Crawford, K., and Schultz, J. (2017). Limitless worker surveillance. Calif. L. Rev., 105, 735.

231 See Ajunwa, I., Crawford, K., and Schultz, J. (2017). Limitless worker surveillance. Calif. L. Rev., 105, 735 referencing Penrose Comput. Marketgrp., Inc. v. Camin, 682 F. Supp. 2d 202, 210-1 1 (N.D.N. Y. 2010)

232 *Computer Fraud and Abuse Act*, 18 U.S.C. § 1030 (1986).

233 Graham, E. (2024, March 20). Lawmakers propose a new federal office to regulate workplace surveillance tech. *Government Executive*. https://www.govexec.com/technology/2024/03/lawmakers-propose-new-federal-office-regulate-workplace-surveillance-tech/395100/

234 *Stop Spying Bosses Act*. 118th Congress. 2nd session. (2024) https://deluzio.house.gov/sites/evo-subsites/deluzio.house.gov/files/evo-media-document/Stop%20Spying%20Bosses%20Bill%20Text%20FINAL.pdf

235 Section 3. Disclosure of Certain Workplace Surveillance s.3(a)(b)(c); s.3(1)(A-G); and s.3(2).

Employees hired five years before, on, or after, the law comes into effect (if it does) would be required to receive disclosure of the employer's policy no later than 30 days after the hiring decision (for new hires), or no later than 60 days after the law comes into effect.[236] Notably, job applicants are obligated to receive this information *prior* to their application being accepted.[237] Any updates to the policy are required to be communicated within seven days.[238] Employers may not use collected data for a purpose that is not disclosed in accordance with these particular rules.[239] Workers are also afforded a right to request and correct data that is held about them, with employers being obligated to provide requested data with seven days of a request being made.[240]

There are also certain prohibitions proposed on workplace surveillance (section 4 of the act). Any collection of employee data by an employer must be reasonably related to the operations of the employer and the employer must restrict access to this information based on "a specific and reasonable business rationale that is proportionate to the need for such access."[241] Additionally, employers — or any third parties that may be contracted to perform the monitoring — may not use workplace surveillance to identify any worker associations or activities associated with "a labour organization" (i.e., union).[242]

Explicit prohibitions are also placed on other aspects of monitoring (except as otherwise protected in law). The bill prohibits using monitoring to access an individual's political or religious beliefs or activities, "or other identify marker … that is unrelated to the performance of the job duties … for the employer."[243] It also explicitly disallows the collection of information about (or to try and determine) an employee's overall health status, any health condition, or an employee's disability status.[244] Again, these restrictions apply unless gathering such health information is directly connected to the employee's ability to perform their job duties. Two other express limitations exist — one that prohibits employers from ascertaining the immigration status of an individual[245] and a whistleblower protection that prohibits employers from using monitoring to track employee's activities relating to reporting the employer (or the third-party contractor) for breaking other laws. The whistleblower provision includes both active monitoring to identify whistleblowers or retroactive use of monitoring tools to determine employees who have made (or intend to make) a report.[246] Section 7 of the bill also provides much more extensive (and explicit) protections for whistleblowers that prohibit employers from engaging in any retaliatory activities against employees, notably, this includes those seeking any assistance with respect to a worker privacy-related concern.[247]

---

236 Bill 88, Section 3(b)1
237 Bill 88, Section 3(b)1
238 Bill 88, Section 3(b)1
239 Bill 88, Section 4(5)
240 *Stop Spying Bosses Act*, Section 3(e)
241 *Stop Spying Bosses Act*, Section 4(d)(2)
242 *Stop Spying Bosses Act*, Section 4 a(1)(A)(B)(C)).
243 *Stop Spying Bosses Act*, Section 4(1)(C)
244 *Stop Spying Bosses Act*, Section 4(1)(D)
245 *Stop Spying Bosses Act*, Section 4(1)(E)
246 *Stop Spying Bosses Act*, Section 4(1)(F)
247 *Stop Spying Bosses Act*, Section 7(2)(B)

Several other provisions limit specific employer behaviours. Specifically, employers cannot use "an automated decision system" to predict an employee's behaviour outside of work, preventing the use of algorithmic management tools that extend beyond the employee's role.[248] Limitations also exist in terms of the scope of monitoring when off-duty or in sensitive areas at work. Simply, employers cannot monitor employees when they are off-duty, in washrooms or locker rooms, in areas provided for breastfeeding, or in areas provided for prayer or other religious activities.[249]

Specific impacts or surveillance-related harms are also invoked in the proposed bill. Specifically, employers must not use workplace surveillance on an employee "in any manner that threatens the mental or physical health of the covered individual."[250]

The bill also addresses the issue of employers sharing (selling, or licensing) employee data with third parties. In a possible nod to the burgeoning data broker market and the risks it poses to employee privacy, the bill prohibits the sale or licensing of data on an employee "to any person" (including a third party or service provider of the employer, except to a government entity or otherwise provided for in law). If law permits, any transfer of employee data must (for "each instance of a transfer"), be disclosed by the employer to the employee in a secure (encrypted) manner, and the employee retains a right to opt-out of any such transfer.[251] Any contracted third-party that is managing the monitoring on behalf of an employer is expressly prohibited from transferring *any* data on an employee.[252] All of the obligations from the bill that are placed on employers must be reflected in contracts with third-party vendors.[253]

Finally, the bill would establish a Privacy and Technology Division in the Department of Labor. The division would house the creation of a number of advisory boards (i.e., a user advisory board, research advisory board, product advisory board, and a labour advisory board). The Privacy and Technology Division would have powers of investigation to ensure compliance with the bill (and its regulations and orders pursuant to it). These powers would include making requests for information and records, or for their preservation, to resolve complaints (which may also include litigation or referral for criminal proceedings).

Regarding penalties, the bill would establish a private right of action for employees or labour organizations negatively impacted by violations of sections 3, 4, or 7. Courts may award successful plaintiffs damages (up to triple the number of actual damages), as well as statutory damages for failure to comply with disclosure requirements (initially up to $500 per impacted employee, with subsequent violations escalating the penalty). For prohibited use of surveillance data (section 4 violations), damages range from $5,000 to $20,000 per instance, increasing to $10,000-$40,000 for repeated violations. Retaliation against whistleblowers (section 7 violations) carries penalties of $5,000-$50,000, escalating to $10,000-$100,000 for repeat offenses. Additionally, courts may provide injunctive relief,

248 *Stop Spying Bosses Act*, Section 4(2)
249 *Stop Spying Bosses Act*, Section 4(3)
250 *Stop Spying Bosses Act*, Section 4(4)
251 *Stop Spying Bosses Act*, Section 4(b)(1)(A)(i) and Section 4(b)(1)(B)
252 *Stop Spying Bosses Act*, Section 4(2)
253 *Stop Spying Bosses Act*, Section 4(e)

equitable relief, and cover litigation costs. The bill also would require (every two years) two reports to Congress: one a study on workplace surveillance and recommendations on how to mitigate harms; the other a report that details information about enforcement activities, specifically enumerating the violations to section 3, 4, and 7 (and the associated results),[254] as well as strategies for enforcement and future recommendations for improving the effectiveness of the newly established Privacy and Technology Division in the Department of Labor.[255]

California[256]

California has recently established a few important acts relating to workplace monitoring, algorithmic management, and employee privacy. This section delves into this emerging legal landscape.

California Privacy Rights Act and the California Consumer Privacy Act

The *California Privacy Rights Act* (CPRA) is a comprehensive data privacy law that was enacted in 2020 as an expansion to the state's *California Consumer Privacy Act* (CCPA). In addition to further strengthening consumers' rights and the constitutional right to privacy, the amendment extended protection from solely consumers to include the collection and use of employee data.[257] While the CPRA and CCPA's full contours are still being decided through ongoing regulations and judicial review, compliance with the statute is required as of January 1, 2023.

Under the CPRA, new requirements are placed on how California employers can collect and use sensitive employee, job applicant, and contractor data. Employers are obligated, "at or before the point of collection," to inform consumers what categories of personal or sensitive information will be collected, "the purposes for which categories of personal information are collected or used, and whether that information is sold or shared."[258] Any collection or use of personal information that goes beyond the originally disclosed purpose without providing updated notice is prohibited.[259] Employers are also obligated to let employees know how long they intend to retain each category of personal information, or if that is not possible, they must have an explicit and reasonably justifiable explanatory criteria that they used to determine this period to limit the retention of any data.[260] Like the proposed *Stop Spying Bosses Act*, these similar provisions extend to the use of third parties that may control the collection of personal information about employees, including that the collection be

254 *Stop Spying Bosses Act*, Section 9(a)(1)(2)

255 *Stop Spying Bosses Act*, Section 9(b)(1)(2)(3)(4)

256 The California Privacy Rights Act of 2020. Proposition 24 in the November 2020 General Election. https://thecpra.org

257 CPRA 2018, s.3(A)(8)

258 CPRA 2018, 1798.100. (a)(1) and 1798.100. (a)(2)

259 CPRA 2018, 1798.100. (a)(1) and 1798.100. (a)(2)

260 Under the CPRA, sensitive information includes "Personal information that reveals: a consumer's social security, driver's license, state identification card, or passport number; a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; a consumer's precise geolocation; a consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership; the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; a consumer's genetic data".

justifiably necessary and proportionate to achieve the purposes for which it was collected. Any entry into a contract that sells or shares personal information for a business purpose must comply with the same level of privacy protection as required in the CPRA.[261]

Additional rights under the CPRA include an employee's right to know / access personal information collected about them (including the categories of third parties that it may be disclosed or sold to),[262] a right to correct personal information,[263] a right to deletion, a right to opt out of the sale or sharing of that information,[264] a right to data portability, a right to limit the use of sensitive personal information,[265] a right to be free from retaliation for the exercise of these rights,[266] and the act introduces accountability measures for the violation of these rights.

In the employment context, the right to deletion appears to be mitigated by an exception if the information is "reasonably necessary for the business, service provider, or contractor to maintain the consumer's personal information in order to"[267] … "enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information."[268]

The CPRA/CCPA does not restrict the use of any workplace surveillance technology, including those that are deemed to be among the most invasive such as EMAs, however, it does provide employees with additional rights when it comes to how their data is collected and used. However, it is the proposed *Workplace Technology Accountability Act*, which would operate in tandem with the CPRA, which introduces much more explicit and detailed obligations surrounding the use of workplace surveillance technologies. Further, there are interesting provisions addressing workplace surveillance in California's 2022 warehouse distributions centers law (AB 701).

Workplace Technology Accountability Act (AB 1651)[269]

California state legislators have also introduced the *Workplace Technology Accountability Act* (AB 1651) 2022, which is currently in the amendment stage. The content of the act has been developed in conjunction with labour unions and worker advocates, and the bill is one of four bills[270] that are currently the strongest worker technology rights proposals in the U.S.[271]

261 CPRA 2018, 1798.100. (d)(2)

262 CPRA 2018, 1798.110. and CPRA 2018, 1798.115.

263 CPRA 2018, 1798.106

264 CPRA 2018, 1798.120.

265 CPRA 2018, 1798.121.

266 CPRA 2018, 1798.125. (a)(1)(E)

267 CPRA 2018, 1798.105. (d)

268 CPRA 2018, 1798.105. (d)(7)

269 This act is also notable for the level of detail provided in its definitions, for example, see *Workplace Technology Accountability Act*, Part 5.6, 1522

270 The others are from Massachusetts (which is modeled on California's AB 1651), and the federal *Stop Spying Bosses Act* (described above) and the No Robot Bosses Act.

271 UC Berkeley Labor Center, Response to the White House Office of Science and Technology Policy (OSTP) Request for Information on Automated Worker Surveillance and Management, June 2023

The following highlights the key policy standards contained in AB 1651 broken down into four sections — worker data rights, accountability in electronic monitoring, algorithms, and impact assessments.

General worker data rights

One of the cornerstones of the act is the provision of a worker right to transparency "at or before the point of collection,"[272] specifically, to "know what personal data are being collected, when they are being monitored, what algorithms are being used, and how the employer will use their data."[273] These requirements apply to both businesses or third-party vendors working on behalf of employers and the level of detail in the notification process is notably striking, including: the specific categories of data to be collected, the purposes, and "whether and how the data is related to the workers' essential job functions."[274] This notice must further include:

- Whether and how the data will be used to make or assist an employment-related decision, including any associated benchmarks.[275]
- Whether the data will be deidentified.[276]
- Whether the data will be used at the individual level, in aggregate form, or both.[277]
- Whether the information is being disclosed or otherwise transferred to a vendor or other third party, the name of the vendor or third party, and for what purpose.[278]
- The length of time the employer intends to retain each category of worker data.[279]
- The worker's right to access and correct their worker data.[280]
- Any data protection impact assessments, and the identity of any worker information systems, that are the subject of an active investigation by the labor agency.[281]

Also notable, employers are required to provide a copy of this notice to the labor agency.[282]

In addition to notice requirements, workers are also afforded a right to access and correct erroneous data in an accessible format at zero cost.[283] Employers, or a vendor working on behalf of an employer as part of the workplace monitoring, data management, or algorithmic management process, must include the following in a response to a request:

- The specific categories and specific pieces of worker data that the employer, or a vendor acting on behalf of the employer, retains about that work.[284]

---

272 *Workplace Technology Accountability Act*, Part 5.6, 1530(a)
273 *Workplace Technology Accountability Act*, Part 5.6, 1521(e)
274 *Workplace Technology Accountability Act*, Part 5.6, 1530(a)(1)
275 *Workplace Technology Accountability Act*, Part 5.6, 1530(a)(2)
276 *Workplace Technology Accountability Act*, Part 5.6, 1530(a)(3)
277 Workplace Technology Accountability Act, Part 5.6, 1530(a)(4)
278 *Workplace Technology Accountability Act*, Part 5.6, 1530(a)(5)
279 *Workplace Technology Accountability Act*, Part 5.6, 1530(a)(6)
280 *Workplace Technology Accountability Act*, Part 5.6, 1530(a)(7)
281 *Workplace Technology Accountability Act*, Part 5.6, 1530(a)(8)
282 *Workplace Technology Accountability Act*, Part 5.6, 1530(d)
283 *Workplace Technology Accountability Act*, Part 5.6, 1521(f)
284 *Workplace Technology Accountability Act*, Part 5.6, 1531(a)(1)

- The sources from which the data is collected.[285]
- The purpose for collecting, storing, analyzing, or interpreting the worker data.[286]
- Whether and how the data is related to the worker's essential job functions, including whether and how the data is used to make or assist an employment-related decision.[287]
- Whether the data is being used as an input in an automated decision system (ADS), and if so, what ADS output is generated based on the data.[288]
- Whether the data was generated as an output of an ADS.[289]
- The names of any vendors or third parties from whom the worker data was obtained, or to whom an employer or vendor acting on behalf of an employer has disclosed the data, and the specific categories of data that was obtained or disclosed.[290]

If a worker believes that data is inaccurate or erroneous, the employer is required to investigate and verify the claim. If the employer discovers that the data is inaccurate, they are required to promptly correct the disputed worker data and inform the employee of the decision. Businesses are also required to review and adjust any employment-related decision or ADS outputs that may have been implicated in the inaccuracy.

AB 1651 also interprets the employment relationship (and employee data) as one context that should be free from the burgeoning data broker industry. For instance, one provision states that employers or a vendor acting on behalf of an employer are prohibited from selling or licensing worker data, "including deidentified or aggregated data, to a vendor or a third party, including another employer."[291]

Even the mere disclosure or transfer of worker data faces restrictions. Specifically, disclosure or transfer cannot occur unless it is pursuant to a contract that requires that the data not be resold or licensed,[292] and unless the transfer will be undertaken through "reasonable security procedures and practices appropriate to the nature of the worker data" to protect the information from unauthorized or illegal access.[293] These security safeguards must consist of "administrative, technical, and physical safeguards."[294] If a breach occurs, a detailed notification about the breach is required.[295]

A number of conditions are placed on categories of data that relate to biometrics, health, and wellness programs. Specifically, biometric, health, or wellness data is prohibited from being transferred altogether, unless it is required under federal or state law.[296] There are also data destruction requirements for biometric, health, and wellness data "when the initial

285 *Workplace Technology Accountability Act*, Part 5.6, 1531(a)(2)
286 *Workplace Technology Accountability Act*, Part 5.6, 1531(a)(3)
287 *Workplace Technology Accountability Act*, Part 5.6, 1531(a)(4)
288 *Workplace Technology Accountability Act*, Part 5.6, 1531(a)(5)
289 *Workplace Technology Accountability Act*, Part 5.6, 1531(a)(6)
290 *Workplace Technology Accountability Act*, Part 5.6, 1531(a)(7)
291 *Workplace Technology Accountability Act*, Part 5.6, 1533(c)
292 *Workplace Technology Accountability Act*, Part 5.6, 1531(d)(1)
293 *Workplace Technology Accountability Act*, Part 5.6, 1531(d)(2)
294 *Workplace Technology Accountability Act*, Part 5.6, 1534(a)
295 *Workplace Technology Accountability Act*, Part 5.6, 1534(b)
296 *Workplace Technology Accountability Act*, Part 5.6, 1533(e)

purpose for collecting the data has been satisfied or at the end of the worker's relationship with the employer."[297] A worker's decision to not participate in a wellness program also cannot be used as a basis for any employment-related decision.[298]

Accountability measures in electronic monitoring

Chapter 3 of the act introduces comprehensive accountability measures for electronic monitoring. These measures are detailed and address various elements to try to ensure that monitoring practices are justified, transparent, and respect workers' rights. These measures include providing: a definition of the allowable purpose,[299] the specific activities, locations, communications, and job roles that will be electronically monitored,[300] the technologies used to conduct the monitoring and the worker data that will be collected,[301] whether the data used will be used to inform an employment-related decision,[302] whether the data gathered through electronic monitoring will be used to assess workers' productivity performance or to set productivity standards, and if so, how,[303] the names of any vendors conducting any monitoring on the employer's behalf and any associated contract language related to that monitoring,[304] a description of a vendor or third party to whom information collected through electronic monitoring will be disclosed or transferred, including the purpose of the sharing,[305] a description of the organizational positions that are authorized to access the data gathered through the specific form of electronic monitoring and under what conditions,[306] a description of the dates, times, and frequency that monitoring will occur,[307] a description of where data will be stored and the length it will be retained,[308] an explanation of why the specific form of electronic monitoring is strictly necessary to accomplish an allowable purpose under the act,[309] an explanation for how the specific monitoring practice is the least invasive means available to accomplish the allowable monitoring purpose,[310] notice of the workers' right to access or correct the data,[311] notice of the workers' right to recourse.[312]

Further specifics about what is contained in the report are spelled out in the act. Notably, the employer disclosure is required to be communicated in a "clear and conspicuous" way, with the act going on to say that "a notice that states electronic monitoring "may" take place or that the employer "reserves the right" to monitor shall not be considered clear and conspicuous."[313] Employers are required to maintain an updated list of any electronic

297 *Workplace Technology Accountability Act*, Part 5.6, 1533(g)
298 *Workplace Technology Accountability Act*, Part 5.6, 1533(h)
299 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(1)
300 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(2)
301 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(3)
302 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(4)
303 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(5)
304 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(6)
305 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(7)
306 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(8)
307 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(9)
308 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(10)
309 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(11)
310 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(12)
311 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(13)
312 *Workplace Technology Accountability Act*, Part 5.6, 1540 (a)(14)
313 *Workplace Technology Accountability Act*, Part 5.6, 1570 and 1571(b)

monitoring systems in use,[314] and any updates or changes in the monitoring must be accompanied by additional notice,[315] as well as a regular provision of notice to workers and the California labor agency on an annual basis.[316]

A set of limits and prohibitions are further established to govern electronic monitoring of workers by employers or vendors carrying out monitoring on their behalf. For instance, employers are permitted to engage in electronic monitoring only if it serves specific allowable purposes which include facilitating essential job functions, monitoring production processes or quality, assessing worker performance, ensuring legal compliance, safeguarding worker health and safety, and managing wages and benefits.[317]

Despite these allowances, explicit minimization limits are imposed on practices that could infringe on worker privacy and rights. Notably, any monitoring must be strictly necessary for the allowable purpose and represent the least invasive means reasonably available to achieve that purpose.[318] Additionally, the specific form of electronic monitoring must be limited to the smallest number of workers and collect only the minimum amount of data necessary to fulfill the allowable purpose.[319] Notably, the act also explicitly disallows any form of electronic monitoring that may lead to labour and employment law violations, that monitors workers outside of duty hours, or that tracks workers to identify those exercising their legal rights, including but not limited to rights enshrined in employment and labour law.[320] Additionally, the use of audio-visual monitoring in highly private areas such as bathrooms, changing rooms, or personal spaces like a worker's residence or vehicle is heavily restricted, except under circumstances critical for ensuring safety or securing data.[321] The incorporation of technologies such as facial recognition or emotion detection in monitoring systems is also prohibited, unless further specified in regulations.[322]

Further worker protections are provided 'upstream' before implementing an electronic productivity system, an employer must submit a system summary to the labor agency, detailing the form of monitoring, the number of workers affected, the data to be collected, and how this data will be used for employment-related decisions. Additionally, the system must undergo review by the labor agency's Division of Occupational Safety and Health to ensure that it does not cause physical or mental harm to workers.[323]

Employers are also restricted from requiring workers to install applications on personal devices that collect or transmit worker data, or to wear, embed, or physically implant those devices, including those implanted under skin or incorporated into clothing or other personal items. Violating these limits is only permitted when absolutely necessary for essential job functions and must be strictly limited to only the specific activities and

314 *Workplace Technology Accountability Act*, Part 5.6, 1542(a)
315 *Workplace Technology Accountability Act*, Part 5.6, 1541
316 *Workplace Technology Accountability Act*, Part 5.6, 1542(b)(1) and 1542 (b)(2)
317 *Workplace Technology Accountability Act*, Part 5.6, 1543(a)1(A-G).
318 *Workplace Technology Accountability Act*, Part 5.6, 1543(2)
319 *Workplace Technology Accountability Act*, Part 5.6, 1543(2)
320 *Workplace Technology Accountability Act*, Part 5.6, 1543(b)(1-3)
321 *Workplace Technology Accountability Act*, Part 5.6, 1543(b)(5)
322 *Workplace Technology Accountability Act*, Part 5.6, 1543(b)(6)
323 *Workplace Technology Accountability Act*, Part 5.6, 1543(c)

times that are necessary to perform essential job functions.[324] Location tracking functions, applications, and devices, for instance, must be disabled when not needed for job-related activities.

Employment decisions in the workplace that rely on data collected through electronic monitoring are also addressed. Employers are prohibited from solely relying on such data for decisions relating to hiring, promotion, termination, or disciplinary actions. Any decision that uses data collected through monitoring must also be independently corroborated with additional managerial documentation.[325] Notably, if the employer is unable to independently corroborate the worker data gathered through monitoring, they are prohibited from relying on that data in making hiring, promotion, termination, or disciplinary decisions.[326] Workers are provided a right to receive the information and judgments that were used in an employer's corroboration or use of monitoring data prior to any decision made about them relating to a hiring, promotion, termination, or disciplinary decision going into effect.[327]

Algorithms

Chapter 4 of the *Workplace Technology Accountability Act* lays out comprehensive requirements for the use of ADS in the work environment.

Notice requirements obligate employers or third-party vendors acting on behalf of employers to inform workers prior to the use of any ADS. In instances where ADSs are already in use, this notice is required within 30 days of the regulations coming into effect.[328] The notice must encompass information on the system's purpose, operational scope, the nature of decisions it influences, applicable benchmarks, types of outputs generated, categories and sources of worker data utilized, as well as details about the system's creators, operators, and the available recourse mechanisms available to workers as outlined in Sections 1570 and 1571.[329] Like the electronic monitoring notification requirements, this section similarly requires that a copy of the notification be forwarded to the California labour agency within 10 days of its distribution to employees.[330] Any significant updates or changes to the ADS or its application must be communicated to employees, underscoring the need for ongoing transparency.[331]

Employers, or vendors working on their behalf, are also required to keep an updated roster of all ADS in operation and to provide an annual update to their workers and the California labour agency of all such systems in use (which must include the same information mentioned above at footnote 258).[332]

Section 1553 outlines restrictions on some applications of ADS in the workplace, explicitly prohibiting their use in ways that violate labour laws, that predict non-job related worker behaviours, that might identify workers that are attempting to exercise their legal rights,

---

324 *Workplace Technology Accountability Act*, Part 5.6, 1543(d)
325 *Workplace Technology Accountability Act*, Part 5.6, 1544(b)
326 *Workplace Technology Accountability Act*, Part 5.6, 1544(b)(2)
327 *Workplace Technology Accountability Act*, Part 5.6, 1544(b)(3)
328 *Workplace Technology Accountability Act*, Part 5.6, 1550(a).
329 *Workplace Technology Accountability Act*, Part 5.6, 1550(b)
330 *Workplace Technology Accountability Act*, Part 5.6, 1550(c)
331 *Workplace Technology Accountability Act*, Part 5.6, 1551
332 *Workplace Technology Accountability Act*, Part 5.6, 1552(b)(c)

that employ controversial technologies like facial, gait, or emotion recognition, use customer feedback as input data, or any other uses deemed harmful by the labor agency in regulation.[333]

The use of ADS outputs is also tightly controlled. Employees' health data cannot be used for employment decisions.[334] This section further establishes that employment decisions must not solely be based on ADS outputs for hiring, promotion, termination, or disciplinary actions. Instead, a 'human-in-the-loop' is required to corroborate ADS outputs.[335] Any decisions employers make using ADS must be transparent, informing affected workers about the rationale behind the decision, any supplementary information used, the specific employee data that was used, the identities of the ADS creators, and any relevant assessments.[336]

Lastly, there are additional accountability measures in place for vendors working on behalf of employers. Notably, vendors are subject to the same regulatory framework as employers, and employers are jointly liable for any compliance failures.[337] Vendors are also tasked with providing all necessary data so that employers can comply with the legislation,[338] and are obligated to return and delete all worker data at the conclusion of their contract.[339]

Impact assessments

And finally, the *Workplace Technology Accountability Act* requires two different kinds of impact assessments — algorithmic impact assessments (AIAs) and data protection impact assessments (DPIAs). Each are dealt with below.

Algorithmic impact assessments

Employers are required to submit algorithmic impact assessments (AIA) of algorithmic information systems and automated decision tools prior to those systems being implemented in the workplace (including retroactive assessments for any ADS already in use).[340] Employers can use a vendor-produced AIA if it complies with the requirements in the *Workplace Technology Accountability Act*.[341]

An AIA is a comprehensive review that identifies potential negative impacts of an ADS on workers. It includes an in-depth examination of the system's design, training data, and functionality.[342] The required components of the AIA include:[343]

- A detailed description of the ADS and its purpose.
- The data types used by the ADS, including input data and training data.

333 *Workplace Technology Accountability Act*, Part 5.6, 1553
334 *Workplace Technology Accountability Act*, Part 5.6, 1554(a)
335 *Workplace Technology Accountability Act*, Part 5.6, 1554(b)
336 *Workplace Technology Accountability Act*, Part 5.6, 1554(b)
337 *Workplace Technology Accountability Act,* Part 5.6, 1555(a)
338 *Workplace Technology Accountability Act, Part 5.6, 1555(b)*
339 *Workplace Technology Accountability Act, Part 5.6, 1555(c)*
340 *Workplace Technology Accountability Act*, Part 5.6, 1521(i) and Workplace Technology Accountability Act, Part 5.6, 1560(a)
341 *Workplace Technology Accountability Act*, Part 5.6, 1560(a)
342 *Workplace Technology Accountability Act*, Part 5.6, 1560(b)
343 *Workplace Technology Accountability Act*, Part 5.6, 1560(b)

- Information on the ADS outputs, their interpretation, and the employment-related decisions they inform.
- An assessment of the ADS's necessity, proportionality, and advantages over non-automated methods.
- A risk evaluation covering errors, discrimination, legal violations, health and safety impacts, chilling effects on legal rights, privacy concerns, economic impacts, and effects on worker dignity and autonomy.
- Measures to mitigate identified risks.
- The methodology for risk evaluation and mitigation.
- Any additional components deemed necessary by the California labor agency.

Data protection impact assessments

For any worker information system (WIS) that an employer develops, procures, uses, or implements, they must also complete a data protection impact assessment (DPIA). Like the AIA, vendor conducted DPIAs are deemed acceptable if they comply with the requirements of the act.[344]

DPIAs, similar in intent to the AIA, scrutinize a WIS for potential negative impacts on workers, focusing on privacy, social, legal, and economic impacts. Specifically, a DPIA must include:[345]

- A systematic description of the WIS, including its scope, context, and purpose.
- An assessment of the WIS's necessity and proportionality.
- An evaluation of potential risks, including legal violations, discrimination, privacy issues, chilling effects on legal rights, impacts on worker dignity and autonomy, and economic or other material impacts.
- Measures to mitigate identified risks.
- The methodology for evaluating risks and mitigation measures.
- Any additional components required by the labor agency.

For both AIAs and DPIAs, assessments must be conducted by an "independent assessor with relevant experience."[346] Interestingly, the process emphasises a co-design approach between employers and workers, requiring that preliminary assessments must be available for anonymous worker review and feedback, with clear protections against retaliation for participating workers.[347] After the consultation process concludes, completed assessments re required to be submitted to both affected workers and the labour agency. In situations where assessments reveal health, safety, discrimination, or bias risks, further submissions to relevant overseers are required (i.e., OHSA for health and safety, and the relevant body overseeing discrimination).[348]

344 *Workplace Technology Accountability Act*, Part 5.6, 1561(a)

345 *Workplace Technology Accountability Act*, Part 5.6, 1561(b)

346 *Workplace Technology Accountability Act*, Part 5.6, 1562(a); Also, note: "independent assessor with relevant experience" is not defined elsewhere in the act.

347 *Workplace Technology Accountability Act*, Part 5.6, 1562(d)

348 *Workplace Technology Accountability Act*, Part 5.6, 1562(e)(1)(2)

An employer may use the ADS or WIS upon submission of the relevant impact assessments to the labor agency unless the labor agency directs otherwise.[349] These additional directions, however, may include requests for additional documentation, further mitigation measures, or prohibition of the system based on the assessment review.[350]

Employers are required to publish a "clear, transparent, and accessible" summary of each impact assessment on their website, detailing methodology, findings, and any changes that they made based on the results.[351] These assessments may be shared with external researchers by the labor agency at their own discretion.[352] Workers, by contrast, are provided a right to anonymously dispute (with the backing of protections cited in Sections 1570 and 1571) the adequacy of AIAs or DPIAs, and to advocate for labor agency investigations into any potential oversights, biases, or perceived failures in independence or completeness.[353] Vendors are also held accountable for adhering to all AIA and DPIA requirements, which includes providing employers with all necessary information for compliance, assisting with assessments or investigations, and sharing joint liability with employers for any instances of non-compliance.[354]

Warehouse distribution centers law (AB 701)

AB 701 is the first U.S. state law of its kind to regulate the use of quotas at warehouse distribution centres. While the law relates to the California Labor Code and not privacy law, the legislation regulates the use of quotas and performance tracking algorithms in large warehouses (i.e., employers who directly or indirectly control 100 or more employees at a single warehouse distribution center or 1,000 or more employees at one or more warehouse distribution centers in California). Employers are required to provide employees with a written notification that includes the description of the quota to be met, the exact number of tasks to be performed or material produced within the defined time period,[355] and any potential adverse employment actions that could emerge from any failure to meet the quota. While AB 701 technically sanctions the use of quotas, it prohibits the use of quotas and performance tracking algorithms that intrude on workers' rights to take appropriate rest/meal breaks, to use bathroom facilities (including reasonable travel time), or that otherwise violate occupational health and safety laws.[356]

Employees may request their personal work data if they believe that meeting a quota prevented them from exercising their rights. This data includes a written description of the quotas they are subject to and a copy of their most recent 90 days of work-speed data (only if the employer collects work-speed data). The employer must provide this information within 21 days.[357] Like the other worker rights legislation in California, provisions exist that protect employees from employer retaliation for requesting information or complaining

349 *Workplace Technology Accountability Act*, Part 5.6, 1562(f)

350 *Workplace Technology Accountability Act*, Part 5.6, 1562(g)

351 *Workplace Technology Accountability Act*, Part 5.6, 1562(h)(i)

352 *Workplace Technology Accountability Act*, Part 5.6, 1562(j)

353 *Workplace Technology Accountability Act*, Part 5.6, 1563(a)

354 *Workplace Technology Accountability Act*, Part 5.6, 1564(a)(b)(c)

355 For example, this includes time-based tasks like processing packages, clearing conveyor belts, and filling containers. (Lab. Code § 2100, subd. (h).)

356 Lab. Code § 2102; see Lab. Code § 2103.

357 Lab. Code § 2104.

about (potentially unlawful) quotas online to authorities,[358] and which allows them to be free from any employer discipline for failing to meet an undisclosed quota.[359]

Illinois

The Illinois *Biometric Information Privacy Act* (BIPA) was one of the first, and is one of the most comprehensive, biometric privacy laws in the U.S. Enacted in 2008 with strong support from the American Civil Liberties Union (ACLU),[360] BIPA defines "biometric information" to include retina or iris scans, fingerprints, voiceprints, hand scans, facial geometry, DNA, and other unique biological markers.[361] The law applies broadly beyond consumers, including to employers collecting biometric data from their employees.

BIPA prohibits private companies (employers included) from collecting biometric data unless they provide written notification to individuals about the specific data being collected or stored. Companies must also disclose the purpose and duration for which the data will be used, and they must obtain written consent from the individual to process biometric data. Additionally, BIPA further establishes standards for how companies must handle biometric information from individuals in Illinois, prohibiting any company from selling this data or profiting from it in any way.[362]

Similarly, the *Illinois Artificial Intelligence Video Interview Act* of 2019[363] complements these protections by requiring employers to notify job applicants if (and how) their video interviews will be analyzed using AI-based assessment tools and to obtain explicit consent from the applicants before implementing such analysis.[364]

New York

New York Local Law 144 presents an early attempt to regulate the potential for harmful biases or discrimination surrounding the use of automated tools in the hiring process.[365] The law specifically targets automated employment decision tools (AEDTs), which are increasingly used by employers to screen and rank job candidates. The legislation requires that AEDTs be subject to an annual bias audit and that the results of these audits, along with a descriptive summary of the tools' development and management processes, be publicly posted.

---

358 State of California Department of Industrial Relations. Report a Labor Law Violation. https://www.dir.ca.gov/dlse/HowToReportViolationtoBOFE.htm

359 (Lab. Code § 2102.)

360 ACLU Illinois. Definition of BIPA. Biometric Information Privacy Act (BIPA). https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa#:~:text=BIPA%20establishes%20standards%20for%20how,profiting%20from%20consumers'%20biometric%20information

361 ACLU Illinois. Definition of Biometrics. *Biometric Information Privacy Act* (BIPA). https://www.aclu-il.org/sites/default/files/field_documents/protect_bipa_5.8.24.pdf

362 Joyce, S. (2024, February 27). BNSF Settles Illinois Biometric Privacy Case for $75 Million. *Bloomberg Law*. https://news.bloomberglaw.com/privacy-and-data-security/bnsf-settles-illinois-biometric-privacy-case-for-75-million

363 Illinois General Assembly. Employment (820 ILCS 42/) *Artificial Intelligence Video Interview Act*. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68

364 Heilwell, J. (2020, January 1). Illinois says you should know if AI is grading your online job interviews. Vox. https://www.vox.com/recode/2020/1/1/21043000/artificial-intelligence-job-applications-illinios-video-interivew-act

365 NYC Consumer Worker Protections. Local Law 144 of 2021. https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page#:~:text=Local%20Law%20144%20of%202021,audit%20is%20publicly%20available%2C%20and

In addition to the audit process, employers are also required to notify candidates at least 10 days before using AEDTs in the hiring process and to notify them of the types of data being collected and how it will be used to facilitate the employment decision. The notification period is designed to give candidates an opportunity to request an alternative evaluation method.

Despite the early adoption of regulations surrounding AEDTs, criticisms are emerging. The law has been criticized as being too weak to make a difference, and research on the 'practical adequacy' of the law is showing that to date, few companies are complying with the requirements.[366]

United Kingdom

In autumn 2023, the U.K. Information Commissioner's Office (ICO) released new guidance for workplace monitoring. The guidance considers new developments in worker datafication, device monitoring technologies, the rise of the gig economy, and remote workplaces.[367]

Aimed at employers to assist compliance with the U.K. *General Data Protection Act* (U.K. GDPR) and the *Data Protection Act* (DPA 2018). These pieces of legislation reflect the positive obligation that is required through U.K.'s compliance with the European Court of Human Rights (ECtHR), which continues to apply in the U.K. post-brexit.

The landmark case of *Barbulescu v Romania* in the ECtHR established that states have a positive obligation to protect employees' Article 8 rights (the right to privacy) within domestic law. Barbulescu presented a detailed framework for balancing employee privacy and employers' legitimate interests in domestic law when it comes to workplace monitoring. The decision noted that that monitoring must be necessary to achieve a specific goal, and that data collection must serve explicit, legitimate purposes. Employers must provide full notification to employees about any monitoring activities. Furthermore, any personal data collected through monitoring must also be proportionate to the stated purpose. Employers are required to implement robust security measures to protect collected data from unauthorized access. And finally, adequate safeguards must be in place, including limiting who can access monitoring data, preventing repurposing or misuse of that data, and deleting it when no longer needed.[368]

Based on this positive obligation, and as domestically expressed through U.K. GDPR and DPA 2018, employers in the U.K. are subject to a comprehensive degree of legal provisions. The following sections outlines them in detail.

366 Weber, L. (2024, Jan 22). New York City Passed an AI Hiring Law. So Far, Few Companies Are Following It. *Wall Street Journal*. https://www.wsj.com/business/new-york-city-passed-an-ai-hiring-law-so-far-few-companies-are-following-it-7e31a5b7

367 U.K. Information Commissioner's Office. (2023) Employment practices and data protection: monitoring workers. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/

368 *Barbulescu v Romania* (2017) 61496/08.

Finding a lawful basis

Employers are required to provide a lawful basis for employee monitoring (and they may choose at least one from among six that are available). Selecting a lawful basis depends on the specific purpose and context of monitoring that employees are subject to. The six lawful bases include:

- **Consent**: the worker must "freely given their consent," although given the power imbalance specific to the employment relationship, this obligation can only be given if "workers have a genuine choice and control over monitoring."[369] Employees are given the option to withdraw consent "without detriment" and employers are required to maintain records about how consent was acquired in an unambiguous and affirmative way.[370]
- **Contract**: That the monitoring is necessary for a contract, such as an employment contract. However, the guidance states that "as monitoring is more often for internal business improvement purposes, it's unlikely that it will be a suitable lawful basis for monitoring workers."[371]
- **Legal obligation**: Employers may rely on the lawful basis of legal obligation if the monitoring is for the purposes of compliance with a common law or statutory obligation (and not contractual obligations). In this case, employers are required to identify the specific legal provision (or equal advice or guidance) that sets out the obligation.[372]
- **Vital interests**: This legal basis relates to data processing that may be necessary to protect an individual's life, sometimes in an emergency. As such, it is limited in scope, and it is very likely another lawful basis would be more suitable.[373]
- **Public task**: While this lawful basis most often applies to public authorities, given the justification of data processing to perform a task in the public interest or for official functions, it may apply to organizations that carry out tasks in support of the public interest, such as a charity working under contract to a public authority to help carry out official functions in the public interest. To use this lawful basis, the basis must be assessed in relation to the specific monitoring activity to ground the appropriate alignment between the monitoring itself and the public interest outcome. This basis also cannot be relied on if the organization could achieve the same purpose in an alternative, less intrusive, manner.
- **Legitimate interests**: The legitimate interest basis implies that the monitoring is necessary for an organization's legitimate interest (or those of a third party if the monitoring is being undertaken on behalf of an organization) unless the risks to workers' rights overrides this interest.

369 U.K. Information Commissioner's Office. Data protection and monitoring workers. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/

370 U.K. Information Commissioner's Office. Data protection and monitoring workers. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/

371 U.K Information Commissioner's Office. Data protection and monitoring workers. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/

372 U.K. Information Commissioner's Office. Data protection and monitoring workers. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/

373 U.K. Information Commissioner's Office. Data protection and monitoring workers. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/

As the most broadly applicable, and most widely used, legal justification for electronic monitoring in the U.K., the legitimate interest requires further analysis. Most notably, the legitimate interest basis does not apply if the monitoring occurs in ways that workers do not understand and would not reasonably expect, or if it is likely that some workers would object if it were explained it to them.[374]

Employers are required to balance their own interests in the monitoring against workers' own interest, rights, and freedoms, under the specific circumstances. A three-part test is required to ascertain this balance,[375] including:

- **Purpose test**: whether there is a legitimate interest behind the processing.
- **Necessity test**: whether the processing is necessary for that purpose.
- **Balancing test**: whether the legitimate interest is overridden by the person's interests, rights, or freedoms.

Processing special category data

The processing of health and biometric data, which forms part of 'special category data' often receives heightened protections. This category of data which includes data revealing or concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification or authentication purposes), health or disability, sex life, or sexual orientation.[376]

If monitoring captures special category data, whether purposefully or "incidentally", employers must obtain both a special category condition as well as a lawful basis, prior to monitoring. If this condition is met, employers must only retain information that is relevant to the monitoring purpose. Additional conditions for processing special category data are several, and those most relevant to the employment context include (but are not limited to): explicit consent (provided an alternative choice for monitoring is given) Article 9(2)(a)), processing pursuant to employment, social security and social protection law to monitor to ensure the health and safety of workers (Article 9(2)(b)), substantial public interest (with a basis in law) to demonstrate wider public interest benefit of "incidental collection" (e.g., special category data is incidentally collected through CCTV crime prevention at a bank), or health or social care (to assess the working capacity of an employee (Article 9(2)(h)).

In order for employers to collect special category data, or to conduct monitoring likely to yield high risk to workers' and other people's interests,[377] however, the employer must undertake a data protection impact assessment (DPIA) and must notify workers about the monitoring in a way that is accessible and easy to understand, as well as about the purpose of monitoring and how the collected information will be used.

374 U.K. Information Commissioner's Office. Data protection and monitoring workers. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/

375 U.K.Information Commissioner's Office. Data protection and monitoring workers. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/

376 U.K. Information Commissioner's Office. Data protection and monitoring workers. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/

377 The U.K. Information Commissioner's Office cites examples of "high risk processing" to include processing biometric data of workers; keystroke monitoring of workers; monitoring that may result in financial loss (such as performance management); or using profiling or special category data to decide on access to services.

Data minimization and deletion principles

Data minimization and data deletion principles must be adhered to, meaning employers must not collect more information than what is needed to fulfill the purpose (for example, no more than what is necessary for reasons of performance, attendance, or security). Data must be deleted (as part of a required retention schedule) once it is no longer necessary for the employer's particular purposes.

The right to data accuracy and access

Data accuracy principles must also be respected. Employers must take all reasonable steps to ensure any collected information is up to date and is not incorrect or misleading. Any discovery that the information is inaccurate obligates employers to take reasonable steps to correct or erase the information. Employees may rely on a subject access request (SAR) to access the personal information that their employer holds about them.[378]

Data security

Data security requirements in U.K. GDPR and U.K. DPA require that employers have appropriate organizational and technical measures in place to protect any personal information that is acquired through monitoring.

Notification requirements

Employers must ensure workers are aware of what personal information is being collected during any monitoring activities, and how this information is being collected. Employers must also keep privacy information up-to-date and inform workers when changes to monitoring practices are introduced.

Recent decisions from the U.K. Information Commissioner's Office

In February 2024, the ICO ordered public service provider Serco Leisure to cease their use of facial recognition technology and fingerprint scanning to monitor employee attendance. The ICO found that Serco failed to show why the use of biometric identifiers are necessary or proportionate for the purpose of attendance, when alternative less intrusive means are available.[379] Following an earlier probe in 2020 by the U.K. ICO, Barclay's Bank subsequently scrapped an employee computer monitoring system that tracked the amount of time that employee's spent at their desks, which sent warnings to those spending too long on breaks.[380]

---

378 U.K. Information Commissioner's Office. Right of access. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/

379 U.K. Information Commissioner's Office. (2024, February 23) ICO orders Serco Leisure to stop using facial recognition technology to monitor attendance of leisure centre employees. *ICO News*. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-orders-serco-leisure-to-stop-using-facial-recognition-technology/

380 Singh, K. (2020, August 9). Barclays being probed by U.K. privacy watchdog on accusations of spying on staff. *Globe and Mail*. https://www.theglobeandmail.com/business/international-business/article-barclays-being-probed-by-uk-privacy-watchdog-on-accusations-of/

Europe

Most of GDPR as it relates to data privacy in the workplace is covered in U.K. GDPR (as U.K. has a positive obligation to uphold GDPR rights), however, there are two important developments in Europe relating to algorithmic management in the workplace that must be reviewed — the *EU Artificial Intelligence Act* (AIA) and the EU rules on platform work.

EU Artificial Intelligence Act

The *Artificial Intelligence Act* (AIA) is the first ever comprehensive legal framework on AI in the world. Agreed among member states in December 2023, it was adopted on March 13, 2024, and aims to uphold the safety and fundamental rights of individuals and businesses regarding AI.[381]

Regulations in the AIA are considered through an incremental risk-based approach, ranging from outright prohibition on certain AI systems that are deemed unacceptable-risk, to rigorous controls on high-risk, which then decrease in degrees of intensiveness from limited-risk to minimal-risk.

Prohibited uses of AI (i.e., unacceptable risk) include those that are designed to surreptitiously influence human behaviour (dark pattern AI), facial recognition in publicly accessible spaces for law enforcement uses (subject to some exceptions),[382] and, most notably for the workplace environment, using biometric information to ascertain a person's race, sexual orientation, beliefs, or trade union involvement.

AI systems defined as high-risk include a range of use contexts, including but not limited to critical infrastructure (transport safety), border control (automating visa applications), educational and vocational training (exam scoring). Importantly, this risk classification also includes employment, worker management, and access to self-employment given their potential for impact on "future career prospects, livelihoods of those persons and workers' rights."[383] Specifically, workplace uses include the use of automated hiring algorithms, productivity scoring algorithms, and any AI system that assists with employment decisions, such as hiring, discipline, or termination.

Obligations surrounding the use of high-risk AI systems in the workplace kick in before specific technological systems can be put on the market. An AI hiring algorithm, for example, must be subject to adequate risk assessment and harm mitigation controls, is subject to certain controls on training data to minimize risks and discriminatory effects, and is required to have appropriate human oversight during their use to minimize risk. This information is required to be clearly communicated to the deployer of the technology (in this instance, where a business relies on a third-party vendors' system). Developers are also required to maintain extensive record keeping, ensuring requirements surrounding accuracy and traceability of results are met, and to ultimately facilitate transparency and accountability to allow authorities to assess compliance.

381 European Parliament News Release. (2023, March 13). *Artificial Intelligence Act*: MEPs adopt landmark law. https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law

382 Workplaces and prisons are not considered publicly accessible spaces, EU AIA, s.19

383 AIA, s.57

Ultimately, any high-risk algorithm used in the workplace will need to undergo a conformity assessment to comply with requirements in the AIA, wherein it will be registered in an EU database, and should it be approved, it will be certified and given a CE marking. Once the product is on the market, however, deployers are still required to ensure human oversight and monitoring, and providers are also required to maintain a "post-market" monitoring system to be able to identify (and report) any incidents of malfunctioning or harm.[384]

The AIA complements existing EU workers' rights. While numerous rights exist (which fall beyond the scope of this report), one notable area is where the AIA addresses AI-driven productivity or performance evaluations. Here, fundamental privacy rights would apply, including the EU GDPR and Article 8 of the ECHR. Additionally, the AIA aligns with Directive 2002/14/EC of the European Parliament and of the Council, which mandates employer obligations to inform and consult employees about workplace decisions, which would appear to include the adoption and use of high-risk AI systems. Member states, however, are responsible for implementing this directive within their own legal frameworks.[385]

EU rules on platform work

The EU has also established rules on the use of algorithms in the workplace that relate most directly to workers in digital labour platforms.[386] [387] In addition to establishing greater access to labour rights for gig economy workers by recognizing their status as being in a formal employment relationship, the new EU rules also directly address the use of algorithms in the workplace. Under the new rules (and perhaps supplementing Directive 2002/14/EC noted above), workers are required to be notified about the use of automated monitoring and decision-making systems.[388] Furthermore, digital labour platforms will be prohibited from collecting, using, and disclosing certain types of personal data, such as: personal data on the emotional or psychological state of platform workers, data related to private conversations, data to predict actual or potential trade union activity, data used to infer a worker's racial or ethnic origin, migration status, political opinions, religious beliefs, or health status, as well as biometric data (other than what might be used for authentication).[389] Human oversight and evaluation are also required in situations where automated decision making is implicated, including workers' right to have any decision made transparent, explained, and reviewed.[390]

---

384 European Commission. (2024, 6 March). https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

385 Directive 2002/14/EC of the European Parliament and of the Council

386 Council of the European Union. Policies: EU rules on platform work. https://www.consilium.europa.eu/en/policies/platform-work-eu/

387 Aloisi, A. (2022, October 1). Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights. *International Journal of Comparative Labour Law and Industrial Relations*, 40(1), 37-70. SSRN: https://ssrn.com/abstract=4235261

388 Council of the European Union. Policies: EU rules on platform work. https://www.consilium.europa.eu/en/policies/platform-work-eu/

389 Council of the European Union. Policies: EU rules on platform work. https://www.consilium.europa.eu/en/policies/platform-work-eu/

390 Council of the European Union. Directive of the European Parliament and of the Council of Europe on Improving Working Conditions in Platform Work. https://data.consilium.europa.eu/doc/document/ST-7212-2024-ADD-1/en/pdf (March 8, 2024)

Lessons from emerging legislative approaches

This sub-section outlines key lessons from the various legal regimes analyzed above. While different jurisdictions choose their own unique approaches, the examples above provide samples of mechanisms and areas of focus that contribute to robust legislative models designed to ensure strong workplace monitoring, algorithmic management, and employee privacy protections.

Broader scope of protection, not just notification, for employees

An emphasis on notification seems insufficient on its own as an employee privacy mechanism. Instead, actual restrictions on employer practices are used in various jurisdictions, which can include restrictions on the types of data that can be collected (see California) as well as requirements for clear definitions and limits on monitoring in sensitive places, (e.g., washrooms, meeting areas) and on the use of specific surveillance technologies (or biometric data, with narrow, well-defined exceptions).

Data minimization and purpose limitation

The assessed examples also indicate that data collection by employers be limited to what is necessary and directly relevant to the employment. This limitation often involves assessing a legitimate interest or business activity against a test (such as the U.K. ICO's three-part test) to balance employer interests in monitoring against workers' own interests, rights, and fundamental freedoms under the specific circumstances. Such tests typically include:

- A purpose test (whether there is a legitimate interest)
- A necessity test (whether the monitoring and processing are necessary for that purpose)
- A third balancing test that asks whether the legitimate interest is overridden by an employee's interests, rights, or freedoms.

This process can involve evaluating whether monitoring occurs in ways that are unexpected or unclear to workers, or if it might reasonably lead to objections on behalf of employees if it were explained to them. Restrictions on collected data are also frequently observed, often with strict penalties for using data beyond its original collection purpose.

Algorithmic transparency and accountability

Requirements for employers to be transparent about the use of algorithmic decision-making tools at all stages of the employment process are also included in various legislative schemes. Employers can be required to disclose the use of algorithms during recruitment / hiring, task assignment, performance, discipline, or termination (and provide potential options for alternative choices to be made). Mandatory disclosures about an algorithm's functioning (through impact assessments), the data used (including where it was sourced), the impact of algorithms on employment decisions, as well as about the identification of biases and associated risk mitigation measures are sometimes required. Regular audits with disclosures to relevant regulatory bodies can also serve a purpose in these schemes Both

the EU *AI Act* and the various relevant laws in California demonstrate these possibilities for ensuring meaningful transparency beyond mere notification.

A robust regime for employee data rights

Workers' rights surrounding electronic monitoring and algorithmic management are often accompanied with a robust regime that allows them to access data collected about them (e.g., through subject access requests), correct inaccuracies in their data, and request data deletion where appropriate. Furthermore, a strong, ongoing notification system is an important complement to these rights, as notifications provide clear, actionable information that enables employees to meaningfully exercise their fundamental rights.

Robust enforcement mechanisms

Effective legislative schemes also seem to recognize that rights without enforcement are meaningless. To give employee rights material impact, strong enforcement mechanisms often include significantly higher penalties for violations to deter non-compliance; a dedicated oversight authority with the power to initiate its own investigations to enforce regulations; and secure, anonymous reporting mechanisms (backed by penalties for employer violation) to protect employees from retaliation. A comprehensive model that properly pairs enforcement mechanisms with worker rights and employer obligations appears far more effective than a patchwork approach that does not pay attention to ensuring the possibility of enforcement.

Complainant and whistleblower protections

The pervasiveness of electronic monitoring and algorithmically inferred behavioural analytics often stresses existing whistleblower protections. New legal approaches therefore recognize that employees who report illegal or unethical practices (including excessive monitoring, privacy violations, or algorithmic biases) need robust legal safeguards aligned with standards like those in the U.S. *Stop Spying Bosses Act*. These protections can include anonymous reporting mechanisms to shield employees from retaliation and strict prohibitions on any form of retaliation against complainants or whistleblowers, with severe penalties for violations.

Protection of union activities

Workplace surveillance and algorithmic systems pose unique threats to the privacy of employees engaged in union activities. While relevant protections extend beyond privacy rights into the realm of labour rights (and therefore beyond the scope of this report), in some legal regimes employers are strictly prohibited from using monitoring technologies, training data, and algorithmic inferences to target union activities. When developing privacy legislation strong examples show that lawmakers and regulators should consult extensively with trade unions across various sectors to ensure robust protections for workers' rights to organize.

Appendix 1: Definitions

The definition of personal information in the Ontario workplace

The Ontario *Freedom of Information and Protection of Privacy Act* (FIPPA)[391] and the Ontario *Municipal Freedom of Information and Privacy Act* (MFIPPA)[392] (the acts) define "personal information" as "recorded information about an identifiable individual." Recorded information includes a range of formats such as electronic records, images, videos, maps, or paper documentation. Information is "about an identifiable individual" if that information "is about an individual in a personal capacity; that is, it reveals something of a personal nature about the individual," and "it is reasonable to expect that an individual can be identified from the information (either alone or by combining it with other information). The kinds of information that are defined as personal information (as recorded information about an identifiable individual) often includes:

a. information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation, or marital or family status of the individual,

b. information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

c. any identifying number, symbol or other particular assigned to the individual,

d. the address, telephone number, fingerprints or blood type of the individual,

e. the personal opinions or views of the individual except where they relate to another individual,

f. correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

g. the views or opinions of another individual about the individual, and

h. the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

The boundary between what does and does not constitute personal information in an employment context, however, is unclear and context-dependent in the acts. An individual's name, title, contact information, or designation that identifies a person in a business, professional, or official capacity (including business that is carried out in a home) is not considered to be personal information. However, when, or if, this personal information "reveals something of a personal nature about the individual," it rises to the level of "personal information" in the acts.

391 *Freedom of Information and Protection of Privacy Act* https://www.ontario.ca/laws/statute/90m56

392 *Municipal Freedom of Information and Protection of Privacy Act* https://www.ontario.ca/laws/statute/90m56

The definition of personal health information and its relationship to work[393]

Personal health information means identifying information about an individual in oral or recorded form, if the information:

- relates to the physical or mental health of the individual, including information that consists of the medical history of the individual's family;
- relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual;
- is a plan of service within the meaning of the *Long-Term Care Act* for the individual;
- relates to payments or eligibility for health care in respect of the individual;
- relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance;
- is the individual's health number; or
- identifies an individual's substitute decision-maker.

393 Cavoukian, A. 2004. *A Guide to the Personal Health Information Protection Act. Information and Privacy Commissioner of Ontario*. https://www.ipc.on.ca/en/resources-and-decisions/guide-personal-health-information-protection-act.

Surveillance and Algorithmic Management at Work: Capabilities, Trends, and Legal Implications