ALEXANDRA MATEESCU AIHA NGUYEN

Explainer: Workplace Monitoring & Surveillance

DATA& SOCIETY

CONTENTS

Executive Summary

New technologies are enabling more varied and pervasive monitoring and surveillance practices in the workplace. This monitoring is becoming increasingly intertwined with *data collection* as the basis for surveillance, performance evaluation, and management. Monitoring and surveillance tools are collecting new kinds of data about workers, enabling quantification of activities or personal qualities that previously may not have been tracked in a given workplace—expanding the granularity, scale, and tempo of data collection. Moreover, workplace monitoring and surveillance can feed automated decision-making and inform predictions about workers' future behaviors, their skills or qualities, and their fitness for employment. Monitoring and surveillance can shift power dynamics between workers and employers, as an imbalance in access to worker data can reduce negotiating power.

This explainer highlights four broad trends in employee monitoring and surveillance technologies:

Prediction and flagging tools that aim to predict characteristics or behaviors of employees or that are designed to identify or deter perceived rule-breaking or fraud. Touted as useful management tools, they can augment biased and discriminatory practices in workplace evaluations and segment workforces into risk categories based on patterns of behavior.

- **Biometric and health data** of workers collected through tools like wearables, fitness tracking apps, and biometric timekeeping systems as a part of employer-provided health care programs, workplace wellness, and digital tracking work shifts tools. Tracking non-work-related activities and information, such as health data, may challenge the boundaries of worker privacy, open avenues for discrimination, and raise questions about consent and workers' ability to opt out of tracking.

- **Remote monitoring and time-tracking** used to manage workers and measure performance remotely. Companies may use these tools to decentralize and lower costs by hiring independent contractors, while still being able to exert control over them like traditional employees with the aid of remote monitoring tools. More advanced time-tracking can generate itemized records of on-the-job activities, which can be used to facilitate wage theft or allow employers to trim what counts as paid work time.

- **Gamification and algorithmic management** of work activities through continuous data collection. Technology can take on management functions, such as sending workers automated "nudges" or adjusting performance benchmarks based on a worker's real-time progress, while gamification renders work

activities into competitive, game-like dynamics driven by performance metrics. However, these practices can create punitive work environments that place pressures on workers to meet demanding and shifting efficiency benchmarks.

Introduction: How is Workplace Monitoring and Surveillance Changing?

New technologies are enabling more varied and pervasive monitoring and surveillance practices in the workplace. This monitoring is becoming increasingly intertwined with *data collection* as the basis for surveillance, performance evaluation, and management. Monitoring and surveillance tools are collecting new kinds of data about workers, enabling quantification of activities or personal qualities that previously may not have been tracked in a given workplace. Employers may seek to quantify "soft" skills such as sociability through tools like facial recognition and sentiment analysis. And employer-provided biometric health trackers may collect sensitive data about workers, from stress levels to smoking habits, raising questions about both consequences at work and growing intrusion into personal life.

Technologies are also enabling employers to expand the granularity, scale, and tempo of data

collection. Data collected about workers are often fed into systems to inform automated decision-making, to make predictions about workers' future behaviors, their skills or qualities, as well as their promotion or continued employment. As Adler-Bell and Miller point out, "data-mining techniques innovated in the consumer realm have moved into the workplace."[1] This can alter the power dynamics between workers and employers, as data-driven decision-making can make management more opaque and difficult to interrogate or challenge. Predictive analytics and flagging tools meant to identify rule-breaking can augment biased and discriminatory practices in workplace evaluations and segment workforces into risk categories based on patterns of behavior—such as identifying which employees are mostly likely to leave their jobs. While these tools are touted as bringing greater insight into workforces through a growing array of metrics, workers and others are challenging the power imbalances they generate, as well as their accuracy and fairness on a technical level.

Moreover, the erosion of worker pay, benefits, and standard protections is a concern where granular tracking of work activities can be used by employers as a cost-cutting tool. Tracking tools, for example, can generate itemized records of on-the-job activities, which

1. Adler-Bell, Sam and Michelle Miller. "The Datafication of Employment," *The Century Foundation*, December 19, 2018, https://tcf.org/content/report/datafication-employment-surveillance-capitalism-shaping-workers-futures-without-knowledge/.

can be used to facilitate wage theft or allow employers to trim what counts as paid work time, excluding "unproductive" periods like down-time. Additionally, algorithmic management and remote monitoring technologies can make it easier for employers to classify workers as independent contractors while still exerting significant control over work processes.

Finally, the growing quantification of work activities can impact job quality and workers' sense of autonomy and discretion in the workplace. For instance, continuous data collection can be used to gamify work—that is, introduce competitive, game-like mechanisms—which can in turn place excessive pressures on workers to meet demanding efficiency benchmarks. And where performance evaluations are increasingly tied to metrics, activities that are most readily machine-readable can become the basis for what counts when work is evaluated, while potentially excluding activities and skills that are less easily quantified.

Grasping the role played by technology is complicated by the wide range of motivations behind why employers monitor workers. Surveillance is usually multipurpose, and the same technologies can be used for both positive and detrimental ends. Monitoring and surveillance tools may serve purposes such as protecting assets and trade secrets, managing risk, controlling costs, enforcing protocols, increasing worker efficiency, or guarding against legal liability. Third-party actors, like

technology companies, may have longer-term interests in using data collected about workers' activities to build technologies that automate tasks.

But outside of employers' own capacity and discretion, there are few legal protections to limit monitoring and suveillance in the workplace, and formal restrictions often must be explicitly built into work agreements, such as through contracts. Norms and expectations of privacy in the workplace also differ significantly across industries, within organizational hierarchies, and across different types of work. As technology helps to render data collection and monitoring and surveillance practices to become cheaper, more efficient, and increasingly pervasive, labor advocates must articulate new limits and strategies for contending with a changing landscape of surveillance.

This explainer highlights four broad trends in employee monitoring and surveillance technologies and discusses some of their implications.

Prediction and Flagging Tools

Technology that aims to predict characteristics or behaviors of employees, flag patterns of behavior, and deter perceived rule-breaking is a growing part of the workplace. While longstanding surveillance tools like CCTV cameras have served similar functions, the

automation of reviewing surveillance data has accelerated the ability to flag and categorize workers based on their perceived risk to employers. Similar to predictive tools within criminal justice and policing contexts,[2] monitoring and surveillance tools can frame workers as potential internal threats to be measured through risk scores, flagging mechanisms that alert to suspicious behavior, and other digital reputation profiling. These tools create the potential for abuse and raise issues around accuracy and use of proxies for behavior and unfair profiling and discrimination.

Risk scoring is commonly used in recruitment technologies across the hiring process, from sourcing to candidate selection. Unlike older forms of vetting like background checks that seek out criminal records, these tools typically flag candidates based on less well-defined categories, often drawing on unconventional information sources like job candidates' online social media activity or emotional cues during interviews. For example, some recruitment technology firms specialize in analyzing job applicants' speech tone and facial expressions in video interviews.[3] Another online service called Predictim, which provides vetting for domestic services, claims

2. Brayne, Sarah. "Big Data Surveillance: The Case of Policing," *American Sociological Review* 82, no. 5 (October 1, 2017): 977–1008, https://doi.org/10.1177/0003122417725865.

3. Zetlin, Minda. "AI Is Now Analyzing Candidates' Facial Expressions During Video Job Interviews," *Inc.*, February 28, 2018, https://www.inc.com/minda-zetlin/ai-is-now-analyzing-candidates-facial-expressions-during-video-job-interviews.html.

to use "advanced artificial intelligence" to analyze a job candidate's personality by scanning their social media posts. The service then generates profiles that list identified traits like "bad attitude."[4] The service's use of social media posts as a measure of employability prompted public backlash, which led to the company halting its launch.[5] In addition to concerns over privacy, Predictim and other predictive models used in the hiring process can reflect biases even when factors like race, gender, or age are explicitly omitted: for instance, work tenure can be correlated with how close a worker lives to their place of employment, but this factor is also strongly correlated with race.[6]

Efforts to predict with data extend beyond vetting and hiring, enabling ongoing review of workers based on a wide range of variables.[7] "People analytics" tools within HR management software are used to

4. Harwell, Drew. "Wanted: The 'Perfect Babysitter.' Must Pass AI Scan for Respect and Attitude.," *Washington Post*, November 23, 2018, https://www.washingtonpost.com/technology/2018/11/16/wanted-perfect-babysitter-must-pass-ai-scan-respect-attitude/.

5. Harwell, Drew. "AI Start-up That Scanned Babysitters Halts Launch Following Post Report," *Washington Post*, December 14, 2018, https://www.washingtonpost.com/technology/2018/12/14/ai-start-up-that-scanned-babysitters-halts-launch-following-post-report/.

6. Bogen, Miranda and Aaron Rieke. "Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias," *Upturn*, December 2018, https://www.upturn.org/reports/2018/hiring-algorithms/; p. 8.

7. Weber, John. "Should Companies Monitor Their Employees' Social Media?" *Wall Street Journal*, October 23, 2014, http://www.wsj.com/articles/should-companies-monitor-their-employees-social-media-1399648685.

predict future behaviors, such as when and whether an employee is likely to leave their job,[8] and have been used by major employers like Walmart.[9] Although less widespread, facial recognition and voice analysis technologies are also used in some areas of job recruiting and customer service, claiming to provide interpretive insight into workers' emotions, social interactions, and "soft skills."

Within knowledge work and white-collar office environments, flagging tools are typically deployed through employer-provided IT systems, such as monitoring and surveillance software used to record computer activities like keystrokes, browsing histories, file downloads, and email exchanges. In many instances, these tools do not enable direct human monitoring but are automated systems designed to flag specific behavioral patterns. One surveillance product, for instance, claims to identify when an employee is distracted and not working efficiently, based on how frequently they

8. Taube, Aaron. "How This Company Knows You're Going To Quit Your Job Before You Do," *Business Insider*, November 19, 2014, https://www.businessinsider.com/workday-predicts-when-employees-will-quit-2014-11.

9. Silverman, Rachel Emma and Nikki Waller, "The Algorithm That Tells the Boss Who Might Quit," *Wall Street Journal*, March 13, 2015, https://www.wsj.com/articles/the-algorithm-that-tells-the-boss-who-might-quit-1426287935.

switch between computer applications.[10] In some cases, these tools are not efficiency oriented but seek to flag "suspicious activity" aimed at protecting intellectual property or preventing data breaches—such as one software product that alerts a manager when an employee downloads an atypically large number of company files.[11]

Within service industries like retail and food service, flagging systems are typically tied to point of sale systems, CCTV surveillance, and digital timekeeping systems. Point of sale system metrics, for instance, are used to generate performance reports on both aggregate and individual work data, including performance data such as workers' speed in processing sales transactions. But they are also designed to generate "exception-based reporting," meaning that the goal of surveillance is to single out workers whose data exhibits outlier patterns, such as processing a higher than average number of customer returns. These forms of profiling may then be used to identify "high risk cashiers."[12] Importantly, the behaviors that these systems use to identify rule-breaking

10. Solon, Olivia. "Big Brother Isn't Just Watching: Workplace Surveillance Can Track Your Every Move," *The Guardian*, November 6, 2017, https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology; "Teramind - Overview," *IBM*, November 21, 2018. https://www.ibm.com/us-en/marketplace/7964.

11. Shahani, Aarti. "Software That Sees Employees, Not Outsiders, As The Real Threat," *NPR*, June 16, 2014, https://www.npr.org/sections/alltechconsidered/2014/06/16/322580735/software-that-sees-employees-not-outsiders-as-the-real-threat.

12. Van Oort, Madison. "The Emotional Labor of Surveillance: Digital Control in Fast Fashion Retail," *Critical Sociology*, July 13, 2018, https://doi.org/10.1177/0896920518778087.

are often proxies rather than concrete evidence of fraudulent or rule-breaking activity. As a result, these tools raise concerns over accuracy as well as employees' ability to contest accusations or provide counter-explanations for their actions.

Biometrics and Health Data

New kinds of data unrelated to workplace activity are coming under the purview of employers. Notably, biometric wearables are becoming common tools within both workplace wellness programs and employer-sponsored health care programs. In 2018, for instance, fitness-tracking device Fitbit launched Fitbit Care, a platform aimed at employer programs.[13] In many cases, data from wearables are used as a means to reduce health insurance premiums.[14] High-profile employers, like BP America, have adopted the device for some of their employees in a bid to improve employee health habits while simultaneously persuading insurance companies to reduce their

13. Ramsey, Lydia. "Fitbit's Moving Away from a Simple Step Counter into Health Coaching as It Faces Competition From the Apple Watch," *Business Insider*, September 22, 2018, https://www.businessinsider.com/fitbit-expands-health-platform-for-employers-called-fitbit-care-2018-9.

14. Olson, Parmy. "Wearable Tech Is Plugging Into Health Insurance," *Forbes*, June 19, 2014, https://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/.

rates, at significant savings to the company.[15] However, tracking non-work related activities and information, such as health data, may challenge the boundaries of worker privacy, open avenues for discrimination, and raise questions about consent and workers' ability to opt out of data collection.

Health tracking programs in the workplace have been critiqued as being potentially coercive even if they are opt-in, by pressuring employees to participate or bear penalties such as paying higher costs or being deemed riskier by their employers.[16] This became a galvanizing issue during the 2018 West Virginia teachers' strike, which in part centered around growing health care costs for public employees. Teachers in West Virginia were introduced to Go365, a health app that the Virginia Public Employees Insurance Agency (PEIA) and health insurance company Humana offered to school employees. The app tracked a wide range of physical activity including users' steps and physical location, to accrue points which could be redeemed for various rewards. Users were also asked to submit to the app sensitive information such as their diets, smoking

15. JBort, Julie. "This Company Saved A Lot Of Money By Tracking Their Employees With Fitbits," Business Insider, accessed November 22, 2018, https://www.businessinsider.com/company-saved-money-with-fitbits-2014-7.

16. Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz, "Limitless Worker Surveillance," *California Law Review* 105, no. 3 (June 1, 2017): 735, https://doi.org/10.15779/Z38BR8MF94.

habits, and family medical histories. Although use of the app was opt-in, many school employees felt the data collection to be invasive, tracking activities even when employees were not working. Use of the app also placed a burden of self-reporting onto employees, requiring them to do unpaid work for which the state would largely benefit in cost-savings. Importantly, those who refused to participate in the program would have to pay higher premiums and other costs to their health insurance.[17]

Similarly, corporate wellness programs are incorporating digital health trackers and using wellness benchmarks to gamify health data in the workplace, incentivizing competition between co-workers to engage in fitness-related activities. Some research has shown the ways this form of data collection can place pressure on employees "to create a body that is perceived as productive and worthy," while raising anxieties about how participation in such programs could negatively affect a worker's employability.[18] For instance, workers who cannot keep up with their colleagues may be regarded as a liability by employers. Moreover, as Ajunwa, Crawford, and Schultz have noted, companies that collect and interpret data from wearables "lawfully

17. Gabrielle, Vincent. "The Dark Side of Gamifying Work," *Fast Company*, November 1, 2018, https://www.fastcompany.com/90260703/the-dark-side-of-gamifying-work.

18. Neff, Gina and Dawn Nafus, *Self-Tracking*, 1 edition (Cambridge, Massachusetts: MIT Press, 2016), p. 130.

operate as black boxes, concealing their data sets and the algorithms they use for interpretation."[19] Employers may still have access to this data, raising the potential for employment discrimination based on categories like age, disability, or pregnancy.[20] The tracking of biometric data also brings monitoring and surveillance beyond the realm of traditional work hours, whether through location-tracking outside the workplace or through wellness programs that track areas like mental health and emotional well-being.[21]

The collection of biometric data in the workplace also raises questions about ownership, retention, and uses of this data, as well as whether employers can compel workers to hand over biometric data. Although use of digital health trackers is typically opt-in, other tools like biometric timekeeping software—which use fingerprints or iris scans to verify employee identity—are often mandatory. In the US, more than 50 companies have faced lawsuits over the collection of employee fingerprint data through biometric timekeeping tools.[22] In 2018,

19. Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz, "Limitless Worker Surveillance," *California Law Review* 105, no. 3 (June 1, 2017): 735, https://doi.org/10.15779/Z38BR8MF94.; 766.

20. Ibid, pp. 752-4.

21. Moore, Phoebe V., *The Quantified Self in Precarity: Work, Technology and What Counts*, 1 edition (New York: Routledge, 2017), p. 6.

22. Janofsky, Adam. "Fingerprint-Scanning Time Clocks Spark Privacy Lawsuits," *Wall Street Journal*, January 11, 2018, sec. Pro Cyber, https://www.wsj.com/articles/biometric-time-clocks-spark-a-wave-of-privacy-lawsuits-1515364278.

a class-action lawsuit was filed in Illinois against employer Wendy's for failing to make employees aware of how the company handles biometric data.[23]

Remote Monitoring and Time-Tracking

Many jobs do not take place within a clearly delimited physical workspace, like an office, a store, or a factory. But tools like GPS-location tracking, computer-monitoring software, app-based activity trackers, and remote sensors enable managers or clients to track and manage workers from afar. Importantly, companies may use these tools to decentralize and lower costs by hiring independent contractors, while still being able to exert control over them like traditional employees with the aid of remote monitoring tools.[24] These tools can produce tensions for remote workers accustomed to more autonomy and discretion.

This trend is exemplified notably on digital labor platforms within the "gig" economy. For example, Upwork is a labor platform where freelancers provide

23. Cimpanu, Catalin. "Wendy's Faces Lawsuit for Unlawfully Collecting Employee Fingerprints," *ZDNet*, September 23, 2018, https://www.zdnet.com/article/wendys-faces-lawsuit-for-unlawfully-collecting-employee-fingerprints/.

24. Newman, Nathan. "Reengineering Workplace Bargaining: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in the Workplace," *University of Cincinnati Law Review* 85 (2017): 697.

services like design, coding, and editing work. While workers on these platforms are typically independent contractors, the incorporation of remote monitoring tools can enable both platform companies and clients to exert control over when, where, and how contractors do their work. Upwork offers an opt-in tool called Work Diary, which counts keystrokes, mouse clicks, and periodically takes screenshots of freelancers' computer screens, among other metrics. Clients are then shown an "Activity Meter" that displays minute-by-minute data about a freelancer's work activity.[25] One challenge to this form of monitoring is that work becomes quantified only in terms of what can actually be measured. More intangible activities such as thinking through ideas, planning work processes, or evaluating one's progress cannot easily be measured, raising questions over how certain kinds of work may be devalued or uncompensated because they cannot be remotely measured in the same way as keystrokes.

The granularity of remote tracking can also be used by employers to itemize what activities count as paid work. One example is electronic visit verification (EVV), a practice that has been implemented as a part of Medicaid fraud oversight in paid carework. EVV

25. O'Donovan, Caroline. "This 'Creepy' Time-Tracking Software Is Like Having Your Boss Watch You Every Second," *BuzzFeed News*, August 7, 2018. https://www.buzzfeednews.com/article/carolineodonovan/upwork-freelancers-work-diary-keystrokes-screenshot.

monitors the work hours and activities of personal care and in-home health care aides. EVV typically consists of software tools that use GPS tracking in order to validate when and where care workers have provided billable services to clients, where previously this may have been done through paper forms like time sheets. Although these systems provide the benefit of ensuring that clients receive the services they need, they also create challenges for care workers, by curbing their autonomy, reducing paid work hours, and potentially infringing on their privacy as well as the privacy of their clients.[26] A case study of EVV implementation in the UK also found that because EVV could be used to more closely track when care workers arrived and left clients' homes, or to itemize different work activities, agencies could more conservatively define billable labor time. This has created challenges for care workers because their day-to-day work is difficult to define in traditional terms of productivity and may fluctuate depending on clients' needs.[27]

Electronic time-tracking has become common in recent years, replacing older methods like manual punch clocks or paper forms used to verify when

26. Metcalf, Jacob. "When Verification Is Also Surveillance," *Data & Society: Points,* February 27, 2018, https://points.datasociety.net/when-verification-is-also-surveillance-21edb6c12cc9.

27. Moore, Sian, and L.J.B. Hayes. "The Electronic Monitoring of Care Work—The Redefinition of Paid Working Time." In Moore, Phoebe V., Martin Upchurch, and Xanthe Whittaker, eds., *Humans and Machines at Work: Monitoring, Surveillance and Automation in Contemporary Capitalism*, 1st ed. 2018 edition (Palgrave Macmillan, 2017), p. 120.

workers clock in and out of shifts. Biometrics, including fingerprint and iris scanning, have been introduced to specifically prevent "time theft" – a term used by employers to describe practices like workers clocking in colleagues on their behalf. However, while the touted goal of these systems is to enforce accurate timekeeping, they can also enable bad actor employers to engage in forms of "digital wage theft" by failing to record workers' time on the clock. A 2017 study that investigated 13 commonly used timekeeping software programs found that default software settings on many electronic timekeeping systems automatically rounded down employees' reported time on shift and applied automatic break deductions regardless of whether an employee took a break or not. The result is that, cumulatively, employees' paid time can be reduced significantly.[28] This is one example of how the recordkeeping of employees can be manipulated. Digitizing certain forms of tracking can shift power away from workers and into the hands of employers, who may use design features in bad faith.

Remote tracking tools can also place pressures on workers to perform to metrics at the expense of safety or health. Long-haul truckers are increasingly tracked through "fleet management systems" which can, as Levy

28. Tippett, Elizabeth, Charlotte S. Alexander, and Zev J. Eigen, "When Timekeeping Software Undermines Compliance," *Yale Journal of Law and Technology* 19, no. 1 (January 14, 2018), https://digitalcommons.law.yale.edu/yjolt/vol19/iss1/1.

has shown, undermine efforts to enforce protocols like safety checks because truckers may cut corners on activities that are not tracked, while also absorbing the risks of "external" conditions like bad weather.[29] United Parcel Service (UPS) drivers are met with similarly conflicting incentives through the monitoring tools collectively termed "telematics"—a neologism that combines "telecommunications" and "informatics"—that use sensors and GPS tracking to both ensure that drivers adhere to safety protocols and work as efficiently as possible. These tools track location, braking, when a car door is opened, and even when drivers buckle the safety belt, among other metrics. [30] While much of this tracking is in the name of safety and efficiency, the extensive rules that govern every action can place excessive pressures on drivers to follow protocols exactly or face disciplinary action. Drivers may be held to account to explain every minor deviation from routine, like taking bathroom breaks, or they may be incentivized to cut corners or undermine data collection by jamming or spoofing sensors.[31]

29. Levy, Karen. "The Future of Work: What Isn't Counted Counts," *Pacific Standard*, August 3, 2015, https://psmag.com/economics/the-future-of-work-what-isnt-counted-counts.

30. Benson, Thor. "From Whole Foods to Amazon, Invasive Technology Controlling Workers Is More Dystopian than You Think," *Salon*, February 24, 2018, https://www.salon.com/2018/02/24/from-whole-foods-to-amazon-invasive-technology-controlling-workers-is-more-dystopian-than-you-think partner/.

31. Bruder, Jessica. "These Workers Have a New Demand: Stop Watching Us," *The Nation*, May 27, 2015, https://www.thenation.com/article/these-workers-have-new-demand-stop-watching-us/.

Gamification and Algorithmic Management

Surveillance is an important component of algorithmic management, a term used to describe real-time data collection that feeds into automated or semi-automated decision-making and that is increasingly behind workplace scheduling, performance evaluations, and other decisions about workers.[32] Many workplace monitoring and surveillance technologies take on management functions beyond merely rule enforcement or oversight, such as sending workers automated "nudges" or directives based on their actions or adjusting performance benchmarks based on a worker's real-time progress. One example is within the Uber ridehail platform, wherein drivers' activities are tracked through their phones, including location, acceleration, working hours, and braking habits, and are monitored through their phones.[33] Both individual and aggregate driver data are then used to target incentives to drivers, such as prompting them to travel to "surge" areas where there is higher demand or to drive certain hours. In cases like these, few work rules are communicated

32. For an overview of algorithmic management in other work contexts, see Mateescu, Alexandra. "Explainer: Algorithmic Management in the Workplace," *Data & Society*, February 2019, https://datasociety.net/output/algorithmic-management-in-the-workplace.

33. Alex Rosenblat, "When Your Boss Is an Algorithm," *The New York Times*, October 15, 2018, sec. Opinion, https://www.nytimes.com/2018/10/12/opinion/sunday/uber-driver-life.html.

outright; rather, rules are enforced through indirect and automated means, placing significant burden on workers to decipher how factors like continuously-changing pay rates are determined.[34]

Algorithmic management depends on continuous data inputs. While professions that largely consist of knowledge work or emotional labor have more easily resisted quantification, technology vendors that promise data-driven analysis of everything from workers' facial micro-expressions to their lunch-time social interactions as potential management tools are emerging. One technology company called Cogito provides a product that tracks interactions between call center workers and customers, using voice analysis to "nudge" call agents to adjust their behavior. For example, call agents are shown a heart icon on their screen when the software detects a "heightened emotional state," directing workers to change their tone or approach the conversation differently.[35] As a result, workers' discretion is circumscribed by automated management of client interactions.

Real-time worker monitoring and surveillance can be further used to gamify work—work structured as game-like and competitive, governed by scores, rules,

34. Rosenblat, Alex. *Uberland: How Algorithms Are Rewriting the Rules of Work*, First edition (Oakland, California: University of California Press, 2018), p. 198.

35. Simonite, Tom. "Call Centers Tap Voice-Analysis Software to Monitor Moods," WIRED, March 19, 2018, https://www.wired.com/story/this-call-may-be-monitored-for-tone-and-emotion/.

rewards, and penalties. For example, some employers have introduced electronic scoreboards positioned prominently in workspaces to display workers' progress and speed in real-time and to incentivize competition between workers.[36] Target cashiers, for instance, are shown a screen that keeps a color-coded score based on checkout process speed, and are expected to keep an 88% rating at the "optimum rate."[37] Productivity apps and software designed for the workplace similarly introduce game-like dynamics, such as badges for work tasks and accomplishments, score-based goal setting, and digital dashboards that display employees' progress.[38]

In some work contexts, these kinds of metrics may serve as useful tools for employees, but in others they may be used by employers to enforce high-pressure work environments. Amazon is known for its extensive surveillance of warehouse workers as they move through space and load and unload products; they face the threat of firing or disciplinary action if they do not meet

36. Gabrielle, Vincent. "The Dark Side of Gamifying Work," *Fast Company*, November 1, 2018, https://www.fastcompany.com/90260703/the-dark-side-of-gamifying-work.

37. Mason, Sarah. "High score, low pay: why the gig economy loves gamification," *The Guardian*, November 20, 2018, https://www.theguardian.com/business/2018/nov/20/high-score-low-pay-gamification-lyft-uber-drivers-ride-hailing-gig-economy.

38. Dougherty, Conor and Quentin Hardy, "Managers Turn to Computer Games, Aiming for More Efficient Employees," *The New York Times*, December 21, 2017, sec. Technology, https://www.nytimes.com/2015/03/16/technology/managers-turn-to-computer-games-aiming-for-more-efficient-employees.html.

efficiency benchmarks.[39] In 2018, Amazon prompted public outrage over a patent the company had filed for the use of a wristband tracking device that would provide "haptic feedback" to warehouse workers, steering them to the correct inventory bins and vibrating if workers' hands strayed too far from where they should be.[40] Although this device has not moved beyond the patent stage, Amazon already engages in similar tracking. Warehouse workers carry handheld electronic devices used to scan and locate products, but which also track and evaluate workers' speed and include countdown timers that pressure workers to keep up with speed expectations.[41] In such cases, workplace monitoring and surveillance tools are also used to generate benchmarks in real-time through aggregate performance data.

39. Head, Simon. "Worse than Wal-Mart: Amazon's Sick Brutality and Secret History of Ruthlessly Intimidating Workers," *Salon*, February 23, 2014, . https://www.salon.com/2014/02/23/worse_than_wal_mart_amazons_sick_brutality_and_secret_history_of_ruthlessly_intimidating_workers/.

40. Yeginsu, Ceylan. "If Workers Slack Off, the Wristband Will Know. (And Amazon Has a Patent for It.)," *The New York Times*, October 17, 2018, sec. Technology, https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html.

41. Gabrielle, Vincent. "The Dark Side of Gamifying Work," *Fast Company*, November 1, 2018, https://www.fastcompany.com/90260703/the-dark-side-of-gamifying-work.

Key Issues

Four key issue areas emerge from the examples discussed in this explainer:

Information and power.
As surveillance, data collection, and management become increasingly intertwined in practices like algorithmic management, the motivations and outcomes of workplace monitoring can become increasingly opaque to workers. There is a conflict of incentives between workers' efforts to succeed in a workplace and employers' incentives to maintain the "information advantage" that data collecting technologies can confer.[42] As law professor Frank Pasquale observes, "[i]f workers knew that thirty-three-word e-mails littered with emoticons scored highest, they might write that way all the time."[43] However, workers' inability to shape, contribute to, or interrogate the kinds of data-driven metrics that increasingly inform how they are hired, evaluated, and managed can produce new challenges. Where workers do not have access to the same data, employers may be placed in a

42. Newman, Nathan. "Reengineering Workplace Bargaining: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in the Workplace," *University of Cincinnati Law Review* 85 (2017): 697.

43. Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*, Reprint edition (Cambridge, Massachusetts London, England: Harvard University Press, 2016): 35.

privileged negotiating position, facing workers with reduced bargaining power.

Accuracy and bias.
Workplace monitoring and surveillance produces a plethora of data about workers, much of which is subject to data mining, interpretation, and analysis. In the hiring context, mathematician Cathy O'Neil has critiqued the use of psychometric testing—questionnaires aimed at psychologically profiling job candidates—as "digital phrenology," arguing that there is little evidence to show that these tools provide accurate insights about whether someone is qualified for a job.[44] Similar critiques are being leveraged against analytics tools that claim to derive insights about employees through methods like vocal risk assessment, but which may in fact perpetrate biases against marginalized workers.[45] If a predictive tool identifies an employee as "high risk"—of breaking company rules, of seeking to leave for another job, or simply of getting distracted on the clock—this raises questions about workers' right of appeal to such assessments.

Moreover, the growing scope of surveillance brings new kinds of data under the purview of employers and consequently brings new potential for workplace

44. O'Neil, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, 1 edition (New York: Crown, 2016).

45. Kofman, Ava. "The Dangerous Junk Science of Vocal Risk Assessment," *The Intercept*, November 25, 2018, https://theintercept.com/2018/11/25/voice-risk-analysis-ac-global/.

discrimination. As the example of digital health trackers shows, there is a potential for "function creep" as data collected about workers for one objective (e.g. encouraging workplace wellness) can be repurposed for other uses (e.g. employee discrimination). [46] Surveillance can reveal more information than intended, or can be used to infer sensitive information about employees. The growing ease of monitoring and surveilling areas like workers' social media activity, health habits, physical movements, and social interactions may mean that normative and legal boundaries of workplace privacy are shifting.

Value and compensation.

The kinds of data employers choose to collect, versus what is ignored, can have consequences for what kinds of work are valued, how performance is evaluated, and how work is classified and compensated. In cases such as remote monitoring and electronic time-tracking, the granular tracking of work activities can be used by employers as a cost-cutting tool. Tracking tools, for example, can generate itemized records of on-the-job activities, which can be used to facilitate wage theft or allow employers to trim what counts as paid work time, excluding "unproductive" periods like down-time. Algorithmic

46. Ball, Kirstie. "Workplace Surveillance: An Overview," *Labor History* 51 (2010): 87–106, https://www.tandfonline.com/doi/abs/10.1080/00236561003654776; 92.

management—enabled by remote monitoring technologies—can make it easier for employers to classify workers as independent contractors, excluding them from many protections and benefits afforded to employees. In these ways, increased surveillance can cumulatively shift how work is valued and compensated.

Job quality.
While in some cases monitoring and algorithmic management can serve to augment work by guiding decision-making, the gamification of performance metrics and pervasive tracking can place harmful pressures on workers. For instance, monitoring and surveillance that only seeks to flag mistakes and rule-breaking or to identify the "weakest link" can be used to sort, rank, and cull workforces, leading to pressures to perform to metrics or risk being fired even while meeting formal job requirements. The growing quantification of work activities can also impact workers' sense of autonomy and discretion in the workplace. As the example of remote monitoring technologies shows, extensive rules that govern every action on the job can place excessive pressures on workers to follow protocols exactly, forgo safety to meet efficiency benchmarks, and often absorb the consequences of factors that monitoring and surveillance systems do not account for. Extensive surveillance can create punitive work environments.

Questions to Consider

- As more aspects of work are tracked, what is most readily "machine-readable" becomes the basis for what counts when work is evaluated, potentially excluding actions, skills, and circumstances that are less easily quantified. However, solutions to this problem often entail more surveillance of workers. How do we navigate this tension?

- Often, workplace monitoring and surveillance produces value from aggregate rather than individual worker data. For instance, a worker's performance may be evaluated by comparison to aggregate data of other similarly-positioned workers. How does this affect conceptions around workplace privacy that are individual-based?

- Workplace tracking tools often use a rhetoric of choice and empowerment for employees. Are there ways to set up and frame workplace monitoring and surveillanc so that employees can functionally opt out without consequence, or does the power imbalance of employment preclude this possibility? What are the collective effects of allowing people to individually opt out?

DATA & SOCIETY

Data & Society is an independent nonprofit research institute that advances new frames for understanding the implications of data-centric and automated technology. We conduct research and build the field of actors to ensure that knowledge guides debate, decision-making, and technical choices.

If you wish to support excellence in independent research, kindly visit **www.datasociety.net/donate**. Data & Society offers many channels for philanthropy. To discuss charitable giving, please contact Executive Director Janet Haven at **haven@datasociety.net**.

www.datasociety.net
@datasociety

**DATA&
SOCIETY**