International Journal of Communication 18(2024), 3128-3139 1932–8036/20240005

More Than Monitoring: Grappling With Bossware

Introduction

LUKE MUNN
University of Queensland, Australia

Bossware, or employee-monitoring software, has grown significantly during and after the pandemic to extensively and invasively surveil remote workers. Tracking app use, mouse clicks, and keystrokes through cloud-based systems, it provides a fine-grained portrait of worker activity, quantifying "productivity" and flagging anomalies. Despite its recent rise, scholarly research is limited, necessitating deeper understanding. This Introduction first provides an overview of bossware and discusses its promises and problems. For proponents, it optimizes productivity and bolsters security; for critics, it increases distrust and intensifies pressures on workers. The Introduction then steps through each contribution to this issue: Barili demonstrates how Time Doctor and Teramind amplify competition and distrust; Ye and Zhao study Chinese workers' ambivalent responses and resistances; and Cinque critiques Microsoft Viva, showing how it reframes workers as quantifiable productivity units. The Introduction concludes by stressing the need for interdisciplinary research to address bossware's complex implications for contemporary labor.

Keywords: remote work, artificial intelligence, people management, digital surveillance, contemporary labor, worker well-being

Bossware. Tattleware. Employee Monitoring. People Management. Whatever the term, this software tracks the activity of workers in extensive and often invasive ways. While bossware has existed for years, interest in it ramped up during and after the pandemic, as managers attempted to oversee and control remote workers. Bossware introduces new digital regimes into the workplace, establishes softer and grayer forms of surveillance, and reshapes the everyday experience of workers in fundamental ways. Some services flag "risky" employees; others offer "productivity scores" to management as a tool to optimize their business (Carter, 2021). These techniques undermine confidence, produce anxiety, and damage worker well-being (Ajunwa, 2018; Ball, 2022; ExpressVPN, 2021; Manley & Williams, 2022).

Luke Munn: luke.munn@gmail.com
Date submitted: 2024-6-6

But if the stakes of bossware are clear, its novelty has made it hard to grasp. At the time of this writing, only a handful of studies exist (Lloyd, 2022; Lomborg, 2022; Stegman, Trottier, Hillier, Khan, & Mannan, 2022), and the most referenced research is an early report by the Electronic Frontier Foundation (Cyphers & Gullo, 2020). A more articulated understanding of bossware is needed. How do we situate bossware within a broader context of digital technologies and contemporary labor? How does bossware operate, what does it offer to management, and how does it reframe what work should be? And how do workers respond to all of this? These are the questions this Special Section pursues. Such questions are not merely about filling a disciplinary gap but are foundational for worker understanding and resistance.

The Introduction begins by defining and contextualizing bossware. The second section traces bossware's recent rise, explains the rationale behind its use, and discusses impacts on workers from privacy violations to metric dominance and trust erosion. The third section steps through each of the contributions to the special section in turn, summarizing their insights. I conclude with an emergent research agenda that highlights gaps in knowledge and suggests promising pathways for further exploration.

Definitions and Origins

What is bossware? Bossware is typically defined as software installed on an employee's computer that tracks their mouse clicks, keystrokes, app usage, and other data (WordSense, 2022). Yet, if this definition is useful, it also has issues. First, what: while some forms of bossware have these explicitly invasive features, others appear more tempered, either in promotional language or actual features. As our contributions suggest, mere "productivity tools" can construct a highly articulated profile of worker behavior. Second, who: while a formal "employee" is mentioned here, the rise of more flexible and on-demand forms of labor (De Stefano, 2015) means targets are increasingly casual, contract, or temporary workers. Such workers typically lack the rights and protections enjoyed by the full-time Fordist-style employee. Third: where: while the definition lists software on a computer, the triumph of software-as-a-service (Alnumay, 2020; Ma, 2007) increasingly means that bossware is deployed through cloud-based platforms rather than installed on a worker's device. Workers may not have the authority or technical literacy to alter this—or may not even know they are being tracked. The very definition of bossware, then, highlights the need for a more articulated and expansive understanding of this phenomenon.

In one sense, bossware's framing has been overly simplistic (Corbyn, 2022; Harwell, 2020). Distinct products have been lumped into a catch-all category and presented using attention-getting terms like "spying" and "surveillance." Certainly these platforms and services raise significant issues for privacy, labor conditions, and worker rights, among others. Yet, tarring all products with the same broad brush actually allows firms to dodge critique, dismissing surveillance concerns as broad "myths" (Zubicki, 2022) that fail to account for the particularities of different products. In another sense, bossware can quickly become disparate and incohesive. One bossware database, for example, lists over 550 "labor-focused technology products" (Coworker, 2021, para. 1), from in-house solutions to patents, background check tools, and widespread video conferencing apps. There is no sense here of a shared provenance, purpose, or set of techniques. A sharper conceptualization is needed, establishing commonalities while leaving room for specificities.

Bossware's mainstream emergence was closely tied to COVID-19. Remote work surged in the wake of pandemic lockdowns (Barrero, Bloom, & Davis, 2020), with over 500 million working from home in the second quarter of 2020 (Soares, Bonnet, & Berg, 2021). While this telework provided freedom in some respects, it also highlighted a number of concerning privacy and equality issues (Katsabian, 2020). If restrictions have largely been lifted in the post-COVID era, many workers remain fully or partially remote, making working from home a new normal (Abdullah, Rahmat, Zawawi, Khamsah, & Anuarsham, 2020; Williamson, Colley, & Hanna-Osborne, 2020).

This unprecedented period provided a window of opportunity that allowed surveillance mechanisms to be broadly deployed using security and public health as a rationale. The biological pandemic was also a surveillance pandemic, enabling invasive technologies such as facial recognition, contact-tracing apps, and population tracking to rapidly spread (Lyon, 2021). The crisis was leveraged as an opportunity to colonize new markets, a form of disaster capitalism (Klein, 2007). Together, these shifts established a normalization of surveillance (Maati & Švedkauskas, 2021).

Software companies have jumped on this opportunity, with remote work becoming a new testbed for workplace surveillance (Ball, 2022). AI technologies now underpin a range of tasks, from monitoring productivity to scheduling work and generating content. While pundits tout the productivity gains of this software and services, others warn of negative impacts on labor conditions and worker rights. Whether termed "workforce analytics," "people management," "employee monitoring," or more derisively "bossware," these technologies have received significant attention for their ability to surveil workers in sophisticated and invasive ways (Corbyn, 2022).

Of course, bossware is not entirely novel. The drive to track and optimize work has a long history that stretches back at least two centuries. In the 19th century, Marx (1867/1977) was already documenting employers using deceitful practices to wrangle a few more minutes from their workers. In the early 20th century, Taylor's (1913) system of scientific management intensified and extended this focus on time, efficiency, and productivity. By analyzing gestures, timing jobs, and streamlining processes, Taylor sought to optimize production. While Taylorism has been superseded by more flexible and self-directed management regimes like Toyotism, the drive to perfect productivity persists (Sandberg, 1994).

Bossware thus answers the longstanding desire to quantify and optimize labor processes, a form of Digital Taylorism (O'Neil, 2017) that goes beyond the workplace to establish its regime over a more expansive domain (Sprague, 2007). Post-pandemic, Digital Taylorism captures the algorithmic management and monitoring that increasingly seems to characterize contemporary work (Armano, Leonardi, & Murgia, 2022; Liu, 2022). But if these Taylorist terms historicize bossware, we also see novel elements: the granularity of feedback, the mobility of monitoring (following workers across devices throughout the day), and the powerful ability to assemble this data into "insights" for management.

Rise and Response

Bossware is on the rise. Web searches for employee surveillance software increased 58% since the start of the pandemic (Migliano, 2022). In one survey of 239 U.S. corporations, use of monitoring tools had risen from 30% pre-pandemic to 60% (Hunter, 2021). Another survey of 1250 U.S. businesses echoed this figure, finding that 60% were using monitoring software to track employee activity and productivity (Digital.com, 2022). Company websites provide another metric for bossware's pervasiveness. iMonitor (2022) boasts that over 25,000 companies in 100 countries are using its product, including Volvo, Siemens, and Sony. The market is forecast to grow at 12% per year and be worth $4.5 billion by 2026 (IndustryARC, 2021). Of course, such measures are imperfect. Survey questions may capture a fuzzy definition of monitoring, and websites may inflate their product's uptake. However, together these measures gesture to the growing pervasiveness of bossware.

What drives this rise? Those who monitor employee behavior provide three core reasons: to increase organizational security, reduce corporate liability, and maximize worker productivity (Lasprogata, King, & Pillay, 2004). If some oversight is necessary for good management, problems arise when surveillance encroaches, when timekeeping becomes obsessive, and when regimes undermine trust and control (Ball, 2010). Bossware establishes the conditions for this "function creep" (Kuldova, 2022), where monitoring for legal compliance can easily turn into broader surveillance.

Bossware proponents claim their products drive productivity, surfacing metrics, establishing competition, and flagging underachievers (ActivTrak, 2022; iMonitor, 2022; Teramind, 2022). But productivity is highly contested, a fraught way of understanding and measuring job performance (Gregg, 2018). Bossware tends to equate productivity with activity: mouse clicks, proper app use, tasks logged. Here "what is measured is not the work but the result of work" (Dejours, Deranty, Renault, & Smith, 2018, p. 208). Deep thinking, relational and affective labor, the "extra" tasks that are actually core to the business—none of this is captured. Problematic measures shape management and the work itself. Workers alter practices to hit these measurements, even if they are dysfunctional (Ridgway, 1956). Metrics move from representation to real goal, a phenomenon known as surrogation (Black, Meservy, Tayler, & Williams, 2022). Workers focus not on the product but on the appearance of productivity.

Bossware introduces other problems. Intense monitoring in call centers has been linked to negative well-being, including higher stress, anxiety, and depression (Holman, Chissick, & Totterdell, 2002). In the contemporary workplace, "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" (Manley & Williams, 2022, p. 706). Pervasive monitoring and algorithmic micro-management damages the mental-health of workers (Milmo, 2021), fallout seen firsthand at Amazon, where workers testify to stress, burnout, and trauma from relentless performance-monitoring regimes (Munn, 2022).

For workers, bossware is a concrete threat with real-world fallout. Workers have argued monitoring technologies infringe on privacy, constitute harassment, and form a hostile working environment (Ajunwa, 2018). Regimes of algorithmic governance manufacture suspicion, turning workers

into risks to be mitigated or managed (Kuldova, 2022). Monitoring cultivates an environment where workers are suspect and data provides evidence to prove wrongdoing and enact punishment. In one survey 88% of companies admitted they fired remote workers after monitoring their work (Digital.com, 2022). Yet, if bossware heightens distrust and undercuts worker contributions, bossware has proliferated widely across industries, placing new pressures on workers.

While legal regimes restrict bossware in some ways, these are piecemeal and partial. In Europe, the General Data Protection Regulation (GDPR) is meant to uphold data protection, transparency, fairness, and privacy when deploying technologies. However, the GDPR's effectiveness is hampered by exceptions and by different interpretations across member states (Aloisi & De Stefano, 2022). In the United States, there is a lack of comprehensive privacy regulation and the "particular threat of data surveillance of remote workers falls between the cracks of privacy laws" (Hewitt, 2023, p. 353). In Australia, the Fair Work commission allowed corporations to roll out monitoring in two high profile cases, arguing the benefits outweighed workers' privacy concerns (Russell Kennedy, 2018). "Data privacy law has an extremely limited reach in the workplace, granting employers broad authority to collect and own information collected from workers" (Calacci, 2022, p. 6). In our probusiness environment, corporate imperatives are upheld and worker concerns ignored.

Contributions

This Special Section features three contributions that explore this novel phenomenon.

Platformizing Surveillance

In "The Platformization of Worker Surveillance," Fabricio Barili investigates two popular monitoring products: Time Doctor and Teramind. Time Doctor promises employers it will help them "build a better workforce by the second." Its focus on tracking and logging worker time appears utilitarian or pragmatic rather than controversial. Yet, as Barili notes, building on Marx, labor time is the key hinge where the struggle over labor takes place: Employers want to extract the maximum productivity in the least time; employees push back against this "more with less" mantra. As Barili shows, apps like Time Doctor are far more granular and active than a mere timesheet, tracking software and mouse use and intervening when activity seems to wane. Such metrics are highly individualized but can be socialized across the company through dashboards and charts. Here we see how software can act in subtle ways to undermine solidarity and instill a highly competitive and time-obsessed culture.

Teramind goes even further, presenting itself as a kind of all-in-one surveillance platform for potential clients. With its Swiss-army knife of features, from screenshotting and audio recording to mouse tracking and time logging, Teramind provides management with a fine-grained view of worker activity throughout the day. While each of these affordances in themselves shapes worker conditions in powerful ways, they come together to drive a particular understanding of the worker and work. As Barili states, Teramind's prime directive is the "search for violations." Implicit in the product's pitch is that workers are not to be trusted; management needs to be vigilant and to amass the evidence needed (a behavioral pattern, a time lag, a nonwork app) to punish offenders, re-exert control, and maintain productivity.

As Barili shows, such apps represent the platformization of surveillance. "Bossware leverages the infrastructure facilitated by the digitization of work environments to apply principles of overseeing, monitoring, and surveilling employees." As companies adopt Office, GSuite, and other offerings, work becomes increasingly digitally mediated. Bossware products derive part of their power precisely because they are *not* presented as dystopian surveillance products but instead as an integral layer in this wider infrastructure that ensures productivity and control. Teramind, Time Doctor, and its brethren follow the platform blueprint: They are software-as-a-service that is paid monthly and can be accessed anytime and anywhere, they collect highly granular data and use it to provide clients with "insights," and they do it all through intuitive feature and user-friendly interfaces. In this way, the platformization of surveillance provides a friction-free and "professional" service—and this is precisely what makes it dangerous for those committed to upholding dignified labor conditions and strong worker rights.

Resistance and Ambivalence

In "Knowledge Workers of the Digital World, Unite!" WeiMing Ye and Luming Zhao investigate how Chinese workers perceive information technology and its ability to amplify and intensify surveillance of them. China is a fascinating and illuminating example here, because in many ways it is at the forefront of contemporary labor conditions. Its intensive work culture is exemplified by pop culture terms like "996.ICU," which signal working 9 a.m.–9 p.m. until you land in the intensive care unit. Yet, young Chinese workers have not passively accepted this brutal work ethic but have pushed back in a range of ways and developed their own attitude toward work. To grasp these perceptions, the authors carry out twelve in-depth interviews with a diverse range of workers and also carry out a content analysis of over 3000 posts from workers on the Chinese social network Weibo.

Situated in China's highly regulated and censored environment, these knowledge workers cannot engage in the kind of open activism (strikes, protests, walkouts) usually associated with resistance but must take another route. Recognizing this, Ye and Zhao adopt Scott's (1990) notion of the "hidden transcript": the speeches, gestures, and practices that occur offstage and may either confirm, contradict, or inflect what appears in public. Certainly these are quieter or less exposed practices that take place in forums or on social media. Yet these are also more ambivalent responses that neither fully condemn nor endorse surveillance and the broader regimes of power they are caught within.

Bringing together these interviews and social media posts, Ye and Zhao demonstrate a range of recurring themes from very high work pressure to work-life balance, complicated workplace relationships, and meager remuneration. Workers intervene in surveillance regimes in subtle but significant ways, advocating for disenchantment with technology, carefully calibrating productivity to avoid being either promoted or fired, and stitching together tech hacks to make themselves appear "busy" or "productive" according to platform logics. This work, linking the meaning of work, job crafting, and emotion as analytical concepts, begins to paint a fascinating portrait of how knowledge workers survive (or even thrive) in a technically mediated environment of intense pressure and pervasive monitoring.

The Productive Worker

In "Rise of the Performance and Assessment Filter," Toija Cinque uses her own engagement with Microsoft Viva to investigate how monitoring software remakes the experience of work. As Cinque makes clear, bossware is not an entirely novel phenomenon that emerges from nowhere but is best understood as a conjunction of two historical trends. Enterprise software like Office and Lotus Notes aimed to digitize work, facilitate communication and collaboration, and centralize and streamline business processes. The rise of cloud-based computing in the last two decades has enabled a vast increase in data collection, in processing power, and in interoperability across sites and contexts. While these developments were premised on empowerment and connectivity, bossware demonstrates how easily these architectures and affordances can be instrumentalized toward surveillance and control, undermining the autonomy and agency that was promised to workers. Today's landscape is characterized by "panoptic regimes" that support "audit cultures" and result in "privacy fatigue" among workers.

After collecting Viva material based on her own behavior over several years, Cinque provides some deep reflections on the implications of these tools. First, she notes how constantly recording fine-grained data about work patterns shapes a particular understanding of the worker as "primarily units of productivity, whose performance is amenable to quantification, measurement, and optimization." These technologies and their reframing are not just for management but spill over into workers' own self-monitoring and subsequent recalibration of their practices. Second, she highlights the subtle but significant role that status indicators play in these regimes. Whether "active" or "unavailable" or "busy," these tokens function as markers of presence and commitment to an organization.

Cinque's insights articulate a more nuanced critique of the bossware phenomenon. Surveillance does not appear in some overt "Big Brother" form, but is rather subsumed into everyday platforms and products. This shift has important implications not just for individual workers but for the future of management and for worker solidarity and organization. While bossware's ability to capture the essence of work may be overstated, the adoption of the people-management paradigm across organizations is nevertheless powerful. For this reason, Cinque calls for a "compassionate and ethical methodology in the application and evaluation of digital technologies within organizational paradigms."

Conclusion

Together, these three pieces provide a rich portrait of the bossware phenomenon, showing the powerful affordances and promises that lead employees to adopting it (Barili), how it plays out in subtle and everyday ways, shaping our experience of work (Cinque), and how workers adapt themselves to the new reality of these pervasive regimes, accepting some measures while pushing back against others (Ye and Zhao).

Such a portrait provides a starting point for further research. We might ask, for instance, how these technologies are taken up in different ways across different industries. How might we articulate the relationship between enterprise-level "people management" and the metric-driven "platformization" of work more broadly? What differences and commonalities exist when we look at how bossware is being

rolled out across Global North versus Global South contexts? And how does age, race, gender, and class figure into the perception and response of workers to these regimes? These questions are complex but already gesture to the import and scope of this phenomenon, making them ideal foundations for a future research agenda.

As these contributions and questions show, bossware is a messy and multidimensional object. Far more than software, it is deeply entangled with business models, managerial projects, labor practices, social dynamics, and industrial relations. This multivalent object requires a multivalent approach, melding together frameworks, concepts, and methods in a highly interdisciplinary fashion. Analyzing affordances might use design and user experience research; grasping worker perceptions may mean observation and ethnography; grappling with data collection and privacy could benefit from legal insights. To adequately conceptualize this phenomenon, interventions will need to go beyond any single discipline and marry media and communications with the rich insights from other areas like political science, labor studies, psychology, gender studies, and management studies.

"Software is eating the world," proclaimed Andreessen (2011) over a decade ago. If these words were hubristic, these also seem prescient as we see everyday work practices becoming increasingly digitally mediated. In this sense, to ask if bossware can ever adequately capture the ingenuity, energy, and relationships that we pour into work practices is perhaps the wrong question. Instead, as labor practices become codified and taskified and workers become embedded in landscapes of increasingly granular data collection, we might ask another question: What does work become? As work becomes platformized and precarized, such a question matters for the lives and livelihoods of workers and those genuinely seeking to support them.

References

Abdullah, N. A. A., Rahmat, N. H., Zawawi, F. Z., Khamsah, M. A. N., & Anuarsham, A. H. (2020). Coping with post COVID-19: Can work from home be a new norm? *European Journal of Social Sciences Studies, 5*(6), 61–81.

ActivTrak. (2022). *Work wiser with workforce analytics & productivity insights*. Retrieved from https://www.activtrak.com/

Ajunwa, I. (2018). Algorithms at work: Productivity monitoring applications and wearable technology as the new data-centric research agenda for employment and labor law. *Saint Louis University Law Journal, 63*(1), 21–45.

Alnumay, W. S. (2020). A brief study on software as a service in cloud computing paradigm. *Journal of Engineering and Applied Sciences, 7*(1), 1–15. doi:10.5455/jeas.2020050101

Aloisi, A., & De Stefano, V. (2022). Essential jobs, remote work and digital surveillance: Addressing the COVID-19 pandemic panopticon. *International Labour Review, 161*(2), 289–314. doi:10.1111/ilr.12219

Andreessen, M. (2011, August 20). *Why software is eating the world*. Retrieved from https://a16z.com/why-software-is-eating-the-world/

Armano, E., Leonardi, D., & Murgia, A. (2022). Algorithmic management in food delivery platforms: Between digital Neo-Taylorism and enhanced subjectivity. *Digital Platforms and Algorithmic Subjectivities*, *24*, 87–96. doi:10.16997/book54.g

Ball, K. (2010). Workplace surveillance: An overview. *Labor History*, *51*(1), 87–106. doi:10.1080/00236561003654776

Ball, K. (2022). Surveillance in the workplace: Past, present, and future. *Surveillance & Society*, *20*(4), 455–461. doi:10.24908/ss.v20i4.15805

Barrero, J. M., Bloom, N., & Davis, S. J. (2020). *COVID-19 is also a reallocation shock* (Working Paper 27137). National Bureau of Economic Research. doi:10.3386/w27137

Black, P. W., Meservy, T. O., Tayler, W. B., & Williams, J. O. (2022). Surrogation fundamentals: Measurement and cognition. *Journal of Management Accounting Research*, *34*(1), 9–29. doi:10.2308/JMAR-2020-071

Calacci, D. (2022). Organizing in the end of employment: Information sharing, data stewardship, and digital workerism. *2022 Symposium on Human-Computer Interaction for Work*, 1–9. doi:10.1145/3533406.3533424

Carter, R. (2021, January 15). *Understanding Microsoft productivity score*. Retrieved from https://www.uctoday.com/collaboration/understanding-microsoft-productivity-score/

Corbyn, Z. (2022, April 27). "Bossware is coming for almost every worker": The software you might not realize is watching you. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2022/apr/27/remote-work-software-home-surveillance-computer-monitoring-pandemic

Coworker. (2021, November). *Bossware and employment tech database*. Retrieved from https://home.coworker.org/worktech/

Cyphers, B., & Gullo, K. (2020, June 30). *Inside the invasive, secretive "bossware" tracking workers*. Retrieved from https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers

Dejours, C., Deranty, J.-P., Renault, E., & Smith, N. H. (2018). *The return of work in critical theory: Self, society, politics*. New York, NY: Columbia University Press.

De Stefano, V. (2015). The rise of the just-in-time workforce: On-demand work, crowdwork, and labor protection in the gig-economy. *Comparative Labor Law & Policy Journal*, *37*, 1–36.

Digital.com. (2022, January 31). *6 in 10 employers require monitoring software for remote workers*. Retrieved from https://digital.com/6-in-10-employers-require-monitoring-software-for-remote-workers/

ExpressVPN. (2021). *ExpressVPN survey shows widespread surveillance on remote workers*. Retrieved from https://www.expressvpn.com/blog/expressvpn-survey-surveillance-on-the-remote-workforce/

Gregg, M. (2018). *Counterproductive: Time management in the knowledge economy*. Durham, NC: Duke University Press.

Harwell, D. (2020, April 30). Managers turn to surveillance software, always-on webcams to ensure employees are (really) working from home. *Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance/

Hewitt, B. (2023). Panoptic employment: Remote worker health data under surveillance. *Science and Technology Law Review*, *24*(2), 2. doi:10.52214/stlr.v24i2.11631

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*(1), 57–81. doi:10.1023/A:1015194108376

Hunter, T. (2021, October 4). Here are all the ways your boss can legally monitor you. *Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2021/08/20/work-from-home-computer-monitoring/

iMonitor. (2022). *Employee monitoring software*. Retrieved from https://www.imonitorsoft.com/

IndustryARC. (2021). *Employee monitoring software market research report*. Retrieved from https://www.industryarc.com/Report/19332/employee-monitoring-software-market.html?utm_source=ABnewswire&utm_medium=Pressrelease&utm_campaign=Paidpress release

Katsabian, T. (2020). *The telework virus: How the COVID-19 pandemic has affected telework and exposed its implications for privacy and equality*. doi:10.2139/ssrn.3684702

Klein, N. (2007). *The shock doctrine: The rise of disaster capitalism*. London, UK: Macmillan.

Kuldova, T. Ø. (2022). Artificial intelligence, algorithmic governance, and the manufacturing of suspicion and risk. In T. Ø. Kuldova (Ed.), *Compliance-Industrial complex: The operating system of a pre-crime society* (pp. 115–151). Cham, Switzerland: Springer Nature. doi:10.1007/978-3-031-19224-1_7

Lasprogata, G., King, N., & Pillay, S. (2004). Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stanford Technology Law Review*, *2004*, 1–47.

Liu, H. Y. (2022). Digital Taylorism in China's e-commerce industry: A case study of Internet professionals. *Economic and Industrial Democracy*, *44*(1), 1–18. doi:10.1177/0143831X211068887

Lloyd, A. (2022). COVID-19 and the future of work: From emergency conditions to regimes of surveillance, governance and optimisation. *Journal of Extreme Anthropology*, *6*(2), 1–20. doi:10.5617/jea.9653

Lomborg, S. (2022). Everyday AI at work: Self-tracking and automated communication for smart work. In S. Pink, M. Berg, D. Lupton, & M. Ruckenstein (Eds.), *Everyday automation* (pp. 126–139). London, UK: Routledge.

Lyon, D. (2021). *Pandemic surveillance*. London, UK: Wiley.

Ma, D. (2007, July). The business model of "software-as-a-service." *IEEE International Conference on Services Computing (SCC 2007)*, 701–702. doi:10.1109/SCC.2007.118

Maati, A., & Švedkauskas, Ž. (2021). Long-term prescription? Digital surveillance is here to stay. *Czech Journal of International Relations*, *56*(4), 105–118. doi:10.32422/mv-cjir.1821

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. doi:10.1177/1350508419890078

Marx, K. (1977). *Capital: A critique of political economy* (B. Fowkes, Trans.). London, UK: Vintage. (Original work published 1867)

Milmo, D. (2021, November 11). Algorithmic tracking is "damaging mental health" of UK workers. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2021/nov/11/algorithmic-monitoring-mental-health-uk-employees

Munn, L. (2022). *Automation is a myth*. Stanford, CA: Stanford University Press.

O'Neill, C. (2017). Taylorism, the European science of work, and the quantified self at work. *Science, Technology, & Human Values*, *42*(4), 600–621. doi:10.1177/0162243916677083

Ridgway, V. F. (1956). Dysfunctional consequences of performance measurements. *Administrative Science Quarterly*, *1*(2), 240–247. doi:10.2307/2390989

Russell Kennedy. (2018, September 4). *Enhancing the workplace or an intrusion of privacy? As surveillance technology continues to evolve, so too will the debate*. Retrieved from https://www.russellkennedy.com.au/insights-events/insights/enhancing-the-workplace-or-an-intrusion-of-privacy-as-surveillance-technology-continues-to-evolve-so-too-will-the-debate

Sandberg, A. (1994). "Volvoism" at the end of the road? *Studies in Political Economy, 45*(1), 170–182. doi:10.1080/19187033.1994.11675378

Scott, J. C. (1990). *Domination and the arts of resistance: Hidden transcripts*. New Haven, CT: Yale University Press.

Soares, S., Bonnet, F., & Berg, J. (2021, April 25). *Working from home during the COVID-19 pandemic: Updating global estimates using household survey data*. Retrieved from https://voxeu.org/article/working-home-during-covid-19-pandemic-updated-estimates

Sprague, R. (2007). From Taylorism to the Omnipticon: Expanding employee surveillance beyond the workplace. *Journal of Computer & Information Law*, *25*(1), 1–35.

Stegman, J., Trottier, P. J., Hillier, C., Khan, H., & Mannan, M. (2022). "My privacy for their security": Employees' privacy perspectives and expectations when using enterprise security software. *ArXiv Preprint ArXiv:2209.11878*.

Taylor, F. W. (1913). *The principles of Scientific Management*. New York, NY: Harper.

Teramind. (2022). *Insider threat detection & employee monitoring*. Retrieved from https://www.teramind.co

Williamson, S., Colley, L., & Hanna-Osborne, S. (2020). Will working from home become the "new normal" in the public sector? *Australian Journal of Public Administration*, *79*(4), 601–607. doi:10.1111/1467-8500.12444

WordSense. (2022). *Bossware*. WordSense Dictionary. Retrieved from https://www.wordsense.eu/bossware/

Zubicki, M. (2022, October 20). *The myths and truths of employee monitoring*. Retrieved from https://veriato.com/blog/myths-truths-employee-monitoring/