Surveillance & Society

Expansive and Invasive: Mapping the “Bossware” Used to Monitor Workers

Luke Munn

Volume 22, numéro 2, 2024

Open Issue

URI : https://id.erudit.org/iderudit/1112222ar
DOI : https://doi.org/10.24908/ss.v22i2.16179

Aller au sommaire du numéro

Éditeur(s)

Surveillance Studies Network

ISSN

1477-7487 (numérique)

Découvrir la revue

Citer cet article

Munn, L. (2024). Expansive and Invasive: Mapping the “Bossware” Used to Monitor Workers. *Surveillance & Society*, *22*(2), 104–119. https://doi.org/10.24908/ss.v22i2.16179

Résumé de l'article

“Bossware” is software that monitors workers, tracking their activity and productivity in often hidden ways. This type of software has seen a surge of interest since the start of the pandemic, as managers attempt to retain oversight of workers in remote or distributed conditions. However, “bossware” is not monolithic but highly differentiated, with each product created by specific companies, with specific affordances, for specific purposes. This article thus builds a more articulated portrait of bossware by mapping the landscape. It first defines a schema based on the “expansiveness” and “invasiveness” of this software and maps key products along these two axes. It then develops a bossware typology ranging from spyware through to soft-bossware and productivity-ware, highlighting their differences in terms of data captured, userbases, perceived legitimacy, and existing safeguards. The article concludes by offering several approaches to investigating these technical regimes and stressing bossware as a site of both power and counterpower.

Surveillance & Society

Article

Expansive and Invasive: Mapping the "Bossware" Used to Monitor Workers

Luke Munn

University of Queensland, Australia
uqlmunn@uq.edu.au

Abstract

"Bossware" is software that monitors workers, tracking their activity and productivity in often hidden ways. This type of software has seen a surge of interest since the start of the pandemic, as managers attempt to retain oversight of workers in remote or distributed conditions. However, "bossware" is not monolithic but highly differentiated, with each product created by specific companies, with specific affordances, for specific purposes. This article thus builds a more articulated portrait of bossware by mapping the landscape. It first defines a schema based on the "expansiveness" and "invasiveness" of this software and maps key products along these two axes. It then develops a bossware typology ranging from spyware through to soft-bossware and productivity-ware, highlighting their differences in terms of data captured, userbases, perceived legitimacy, and existing safeguards. The article concludes by offering several approaches to investigating these technical regimes and stressing bossware as a site of both power and counterpower.

Introduction

In an insurance firm in the UK, new software has been installed on all the computers. It tracks the workers' keystrokes, their browsing history, and is constantly recording whatever is on their monitors. The team manager leverages these new features to meticulously monitor the employees, tracking their productivity via exhaustive metrics and detailed dashboards. One worker has had enough and begins to type up a complaint to the executive manager. But before he can even finish and send it, the team manager confronts him: she saw him typing it in real-time (Greybeard 2021).

"Bossware" is software that monitors workers, tracking their activity and productivity in often hidden ways. This type of software has seen a significant uptick in interest during and in the wake of the pandemic, as managers attempt to retain oversight of workers in remote or distributed conditions. Bossware introduces new dynamics for workers, it intensifies regimes of surveillance and oversight that were already present, and it shapes the labor experience in fundamental ways. Some services flag employees who are deemed risky. Others claim to show how industrious workers are and offer these "productivity scores" to management as a tool for optimizing their business (Carter 2021). These techniques undermine confidence and damage worker well-being. In a survey of 2000 remote workers (ExpressVPN 2021), 59% felt stress or anxiety about their employer surveilling their online activity.

The stakes of bossware, then, are clear. And yet its very novelty and rapid development has made it hard to grasp. To date, there has been only a limited number of academic studies on this nascent phenomenon (Lloyd 2022; Lomborg 2022; Stegman et al. 2022), with the most referenced piece being an early report by the Electronic Frontier Foundation (Cyphers and Gullo 2020). A more articulated understanding of bossware is

Munn, Luke. 2024. Expansive and Invasive: Mapping the "Bossware" Used to Monitor Workers. *Surveillance & Society* 22(2): 104-119.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

needed—and this is not merely an academic exercise, but rather foundational for forms of worker understanding and resistance. What are the various forms of bossware? What are their differences and similarities? And what kinds of risks do they pose for workers? These are the questions this article pursues.

The article begins by contextualizing bossware, stressing its recent rise while also highlighting historical precedents. The second section problematizes bossware, outlining a range of issues from privacy intrusion to metric-centric performance and the erosion of trust and worker well-being. The article then turns to the crux of the contribution: mapping the bossware terrain. It develops an intuitive schema and charts many bossware products along these two axes. The article then uses these clusters of products to develop a provisional typology of bossware. The article steps through each type, laying out its key characteristics and the kinds of threat it poses to personal privacy, individual rights, and basic worker freedoms. The article concludes with an emergent research agenda that suggests possibilities for further analysis and highlights several key gaps in knowledge.

Contextualizing Bossware

Remote work has surged in the wake of pandemic lockdowns, leading to millions more workers operating outside of traditional work contexts (Barrero, Bloom, and Davis 2021). It is estimated that 557 million individuals worked from home during the second quarter of 2020 (Soares, Bonnet, and Berg 2021). And while restrictions have largely been lifted in this so-called post-COVID era, some workers have refused to return to the office, creating a situation where working from home is the new normal (Abdullah et al. 2020; Williamson, Colley, and Hanna-Osborne 2020). The COVID-19 pandemic has highlighted a number of concerning issues in terms of privacy and equality in the context of telework (Katsabian 2020).

This unprecedented period provided surveillance advocates with a window of opportunity, a crisis that enabled them to deploy novel tracking mechanisms on populations using security and public health as the stated rationale. In essence, the pandemic was also a pandemic of surveillance, allowing the rapid spread of invasive technologies such as facial recognition, contact-tracing apps, and population tracking (Lyon 2021). Leveraging crises for such lucrative opportunities is not an anomaly, but a repeated pattern that has been labeled disaster capitalism (Klein 2007). In this regard, the pandemic contributed to a dangerous normalization of surveillance (Maati and Švedkauskas 2021).

Software companies have pivoted quickly to take advantage of this mass migration. Remote work has become a new context for workplace surveillance (Ball 2010). AI technologies, for example, are now used in a variety of digitally mediated tasks, from monitoring productivity to scheduling work and generating content. While some tech pundits have celebrated the productivity gains from these products, such software can also have negative impacts on the rights and well-being of workers. “Bossware” or “tattleware” has received attention in news media as a technology that remotely surveils workers in increasingly invasive and articulated ways (Corbyn 2022).

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 offers a starting point, it also has issues. First, the rise of software-as-a-service (Alnumay 2020; Ma 2007) has meant that bossware may take the form of cloud-based platforms rather than installed software. Secondly, while the definition lists employees as the target, the rise of more flexible and on-demand forms of labor (De Stefano 2015) in the last decade means that these targets could easily be casual, contract, or temporary workers. And finally, while the definition suggests bossware can be clearly identified by invasive features, employment monitoring solutions range widely in terms of features: bossware may not always take the form of easily recognisable surveillance. While such issues do not render these definitions irrelevant, they do suggest that a more detailed portrait of bossware is necessary.

By many measures, employee monitoring appears to be on the rise. One company documented that web searches for employee surveillance software had increased 58% since the start of the pandemic (Migliano

2022). In a survey of 239 large corporations in the United States, Gartner found that the percentage using monitoring tools had risen from 30% prior to the pandemic to 60% (Hunter 2021). Another survey of 1,250 businesses in the US echoed this figure, finding that 60% were using monitoring software to track employee activity and productivity (Digital.com 2022). We can also get a hint of bossware's pervasiveness from company websites. iMonitor (2022), for example, boasts that over 25,000 companies in one-hundred countries are using its product, including Volvo, Siemens, NTTData, and Sony. The employee monitoring software market is forecast to grow at 12% per year, reaching a valuation of $4.5 billion by 2026 (IndustryARC 2021). Such statistics are certainly incomplete. What exactly constitutes "employee monitoring," for instance, is fuzzy and is essentially self-defined by companies who answer surveys. However, taken together, web searches, corporate surveys, and industry growth gesture to bossware's emergence and uptake.

In certain jurisdictions, legislative regimes place restrictions on this adoption and deployment of bossware. The General Data Protection Regulation (GDPR) is the strongest example here, a bundle of laws that establish key concepts, standards, and penalties regarding data protection and privacy across European Union states. Yet if the GDPR requires principles like proportionality, fairness, and transparency to be preserved when deploying technologies, Aloisi and De Stefano (2022) stress that its effectiveness has been significantly undermined by a long list of exceptions. In addition, these are interpreted and upheld differently across member states, resulting in patchwork or uneven regulation (Aloisi and De Stefano 2022).

Even these nominal protections fall away when shifting to other jurisdictions. In the United States, for example, Hewitt (2023: 353) notes a lack of comprehensive privacy legislation at the federal level and argues that "the particular threat of data surveillance of remote workers falls between the cracks of privacy laws." In Australia, where this article's analysis was conducted, specific legislation is either absent or favors employers, creating a laissez-faire regulatory system. A country-by-country analysis of employee monitoring legislation found Australia to be one of the easiest countries for companies to legally surveil employees (Nott 2018). Indeed, the Australian Fair Work commission sided with companies in two high profile cases, arguing the benefits outweighed worker privacy concerns and allowing corporates to roll out monitoring technologies (Kennedy 2018).

Together, these findings suggest that, while legislation does exist, it is piecemeal both in its coverage and enforcement. This (lack of regulation) is partially a byproduct of bossware's novelty and the swift pivot to remote work in the pandemic. Regulation struggles to keep pace, a recurring dilemma with fast-moving technology and slow-moving legislative reforms (Moses 2007). But these toothless regimes are also a reflection of a broader pro-business environment. As Calacci (2022: 6) observes, "Data privacy law has an extremely limited reach in the workplace, granting employers broad authority to collect and own information collected from workers." This is a culture where corporate imperatives tend to be upheld while worker concerns are ignored.

Certainly, bossware is not an entirely novel phenomenon. The drive to track and optimize work has a long history that stretches back at least two centuries. Marx (1977 [1867]) wrote of employers obsessed with wringing the maximum labor from their allotted time, squabbling with workers over minutes. In popular writing, the classic precedent given for bossware is Taylorism. This system of scientific management was developed by Fredrick Winslow Taylor (1913) in the early twentieth century and was driven by the need to find the one best way of accomplishing a job. By timing tasks, analyzing gestures, and streamlining procedures, Taylorism sought to optimize the production of any commodity. While Taylorism was eventually superseded by more flexible management regimes like Toyotism, the prime directive of optimizing productivity remained (Sandberg 1994).

Bossware, in this sense, can be understood as a longstanding desire to quantify and optimize labor processes, a form of Digital Taylorism (O'Neil 2017). Indeed, the surge of remote work and working-from-home fulfills the Taylorist dream to break out of the factory or office and establish its optimization regime over a more expansive domain (Sprague 2007). In the pandemic and post-pandemic, Digital Taylorism gained new

currency as a term that captures the algorithmic management and monitoring that increasingly seems to characterize contemporary work (Armano, Leonardi, and Murgia 2022; Liu 2022). However, if Taylorism helpfully historicizes bossware, we also see an array of novel elements in terms of the granular kind of feedback on offer, the mobility of this software (moving with workers on their devices throughout the day), and the ability of AI-driven models to rapidly assemble this vast amount of data into powerful "scores" and "insights." Framing bossware as simply neo-Taylorism overlooks some of these key details.

Problematizing Bossware

Monitoring advocates argue that there are legitimate reasons to monitor employee behavior. While these range from ensuring compliance to reducing hacking, they fall into three core categories: increasing organizational security, reducing corporate liability, and maximizing worker productivity (Lasprogata, King, and Pillay 2004). As Ball (2010) notes, some degree of oversight in the workplace to gather information and recognize performance is necessary for good management; the problems occur when this surveillance encroaches beyond what is reasonable, when time management becomes time obsession, and when these regimes negatively impact control and trust. Recent research has shown how bossware establishes the conditions for this "function creep," where monitoring for legal compliance can easily turn into broader surveillance for the purposes of performance management and labor control (Kuldova 2022).

Whether bossware amplifies the performance of workers is debatable. On their webpages and in their promotional materials, bossware developers assert that their clients achieve significant gains in productivity (ActivTrak 2022; iMonitor 2022; Teramind 2022). Pastel-colored dashboards display every task by every worker, highlighting the overachievers and flagging the laggards. But productivity is a highly contested term, a historically recent and often fraught way of understanding and measuring job performance (Gregg 2019). The deep thinking needed to understand a problem, the reflection needed to identify misconceptions, the affective and relational work needed to communicate well with colleagues—none of this is measured by bossware, which tends to equate app "engagement" and mouse or keyboard "activity" with productivity.

"What is measured is not the work but the result of work," Dejours et al. (2018: 208) stress, a firehose of figures that "give only a distorted and unfaithful picture of the actual work situation." Bossware meticulously tracks metrics and monitors behavior, but such measures can be superficial or incidental—the downstream ripples of work rather than its core essence. The problem is that workers alter their behaviors to hit these measurements, even if they're dysfunctional (Ridgway 1956). Metrics cease to be a representation and become the concrete goal itself, a phenomenon known as surrogation (Black et al. 2022). This is why Dejours et al. (2018: 203) consider measurement a form of domination: workers are forced to stop caring about the quality of the goods or service and must instead focus on making themselves "productive" according to some arbitrary indicator.

The human fallout of bossware can also be seen in other ways. Intense monitoring in call centers has been linked to negative well-being, including higher stress, anxiety, and depression (Holman, Chissick, and Totterdell 2002). A more recent ethnographic study of a contemporary workplace echoed this link, finding that "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 and Williams 2022: 706). Other studies have found that pervasive monitoring and algorithmic micro-management damages the mental health of workers (Milmo 2021). These negative impacts can be witnessed in the stories of workers. Amazon workers, for instance, testify to stress, burnout, and even trauma as a result of relentless digital regimes that monitor and attempt to maximize their performance (Munn 2022).

Recognising these impacts, some workers have argued that monitoring technologies infringe on privacy, constitute harassment, and form a hostile working environment (Ajunwa 2018). In forums, workers subjected to bossware speak about how it creates an atmosphere of mutual distrust. Bossware establishes a situation where the worker is always suspect, concealing or hiding something. Data then provides the

"evidence" confirming what the employer suspected all along. Disturbingly, 88% of companies in a recent survey admitted they fired remote workers as a result of monitoring their work habits (Digital.com 2022). This dynamic resonates with scholarship showing how regimes of algorithmic governance manufacture suspicion, turning workers into risks to be mitigated or managed (Kuldova 2022).

Together these insights suggest that bossware's exhaustive (but always selective) monitoring of metrics is the wrong approach, heightening distrust and developing a distorted portrait of worker productivity. And yet, despite these fundamental issues, the surging demand for bossware has seen it being widely adopted and rapidly proliferated across industries. This spread places new pressures on the post-pandemic worker, and in some cases, has resulted in their termination.

Mapping Bossware

How can we make sense of bossware as a phenomenon? In the nascent literature to date, bossware has typically been framed in a monolithic way (see Corbyn 2022; Harwell 2020; Kosowski 2022). Distinct products have been lumped together into a catch-all category and presented using attention-getting terms like "spying" and "surveillance." This is not to suggest such critical framings are not legitimate. This software does raise significant concerns in terms of privacy, worker rights, and managerial power more broadly. Yet this all-encompassing framing actually allows companies to dodge critique, dismissing surveillance concerns as broad "myths" (Zubicki 2022) that fail to take into account the particularities of specific software.

If over-simplification is one issue, over-complexity is another. Take, for instance, the Bossware and Employment Tech Database by Coworker (2021). This database was developed over the course of the pandemic as new software and surveillance products were rapidly released to cater to the "new normal." Yet if this resource is certainly laudable, the list of over 550 "labor-focused technology products" can easily become overwhelming. Some items are in-house solutions for tech titans like Amazon; others are mere patents that may never be developed into actual products. Products for carrying out specific tasks like background checks (Checkr.com) appear alongside ubiquitous video conferencing apps like Zoom. This treatment results in a bewildering variety of technologies that seem to lack any unifying characteristics. There is no way to compare and contrast products, to get a sense of their key similarities and differences.

What is needed is a schema to help us make sense of the rapidly developing terrain of bossware. Like Marx (2004), I am interested in mapping the distinct forms that surveillance takes—and particularly starting to grasp the kinds of data that are captured and how this information might be instrumentalized against workers. To this end, this article introduces an intuitive mapping schema for employee-monitoring technologies consisting of two axes.

Invasiveness measures the capacity of the software to intrude on the life and privacy of an individual. How is invasiveness measured? Here I draw upon work by Macnish (2015), who aimed to derive a rough measure of intrusiveness. Technologies can encroach more or less on the private life of the worker. Using the example of an employer monitoring an employee, Macnish (2015) asserts that time-keeping would be relatively unintrusive, but placing CCTV cameras in the workplace, and then throughout the building, would increase this intrusiveness, potentially leading to chilling effects, uniform behavior, and other negative impacts. In addition, Macnish (2015) asserts that the kind of information collected by these mechanisms determines their intrusiveness. Collecting metadata, for instance, may provide the location of a call, but collecting data would capture the actual conversation. In the context of bossware, Microsoft Suite captures metadata (e.g., call time), whereas Spyrix captures the raw data of interactions (e.g., call audio). Based on these insights, a product that constantly logs the individual keystrokes of a user—potentially giving away web searches, credit card details, and health records—would score highly on this axis. Conversely, a more constrained product that lacked features like screenshotting, key logging, and access to the camera would score much lower.

Expansiveness measures the broadness of the featureset built into a specific product. According to Apel and Kästner (2009: 1), a feature is a "unit of functionality of a software system that satisfies a requirement, represents a design decision, and provides a potential configuration option." The total featureset, then, is a combination of all the distinct features contained in a piece of software. As a measure, expansiveness resonates with recent interest in the "scope" of electronic performance monitoring, or the number of ways in which monitoring takes place (Ravid et al. 2020). A product that contains time tracking, productivity scores, screen capture, project management, and numerous tools to monitor a workforce would score highly on this axis. Conversely, a product designed purely as a keystroke logger for individuals would score low. In essence, this axis measures how all-encompassing a particular platform or product is. However, rather than being viewed as a product advantage, expansiveness is understood more critically here as the ability of a technology to provide management with a comprehensive array of tracking, indexing, comparison, and administrative mechanisms that seek to encircle the worker.

Such scales are grounded, then, in insights about the particularities of surveillance technologies, and the way these specificities alter the impacts and potential harms on individuals. Granted, these qualities will always be rougher and more subjective than a quantity measurable through an instrument. However, this also makes them more accessible for a wider audience, who can grasp the key foundations for each scale and use it on their own technologies, systems, and situations. These scales thus operate as a kind of heuristic, a simple and intuitive schema widely used in everyday decision-making (del Campo et al. 2016; Gigerenzer and Gaissmaier 2011). Rather than being limited to "experts," a wide variety of public and private stakeholders can apply this schema to real-world issues, highlighting the particularities of technologies and the tradeoffs they require.

After establishing these two axes, a broad array of bossware products were mapped (Figure 1). Product selection aimed to balance popularity and diversity. Popular and widely adopted products such as Teramind, DeskTime, HubStaff, and Toggl Track were included. These products assert they are used by thousands of companies, and they are regularly featured in roundups of the top employee monitoring software (Schooley 2022). Understanding where these influential and industry-leading products are situated is important. However, breadth was also important to gain a full sense of the bossware landscape. For this reason, the mapping included more niche products like Spyrix. This diversity also meant including productivity platforms like Google Workspace and Microsoft 365 that actually contain a number of management and monitoring features but that are typically not considered bossware.

A product's Invasiveness and Expansiveness scores, as discussed above, are closely linked to its featureset. A list of each product's features was drawn from a SurfShark (2022) table that contains sixteen feature categories, from "keylogging" and "screen monitoring" to "audio recording" and "time tracking," amongst others, with a check if the product has this feature and a blank if it does not. In addition, I visited the website of every product, developing a sense of it through advertising copy, screenshots, and demonstration videos. Methodologically this activity combines elements of qualitative content analysis (White and Marsh 2006) with the walkthrough method (Light, Burgess, and Duguay 2018) of understanding digital software. Together this work provides a strong grasp of a particular product's capabilities and indicates its score on the expansiveness and invasiveness axes.

There are four clusters of points from the map that share similar capabilities when it comes to invasiveness and expansiveness. I use these clusters to develop a provisional typology of bossware composed of four distinct types: spyware, totalware, soft bossware, and productivity ware (Figure 2). In the following sections, I introduce each type, provide an example product, and then discuss the issues and risks it raises in relation to work.

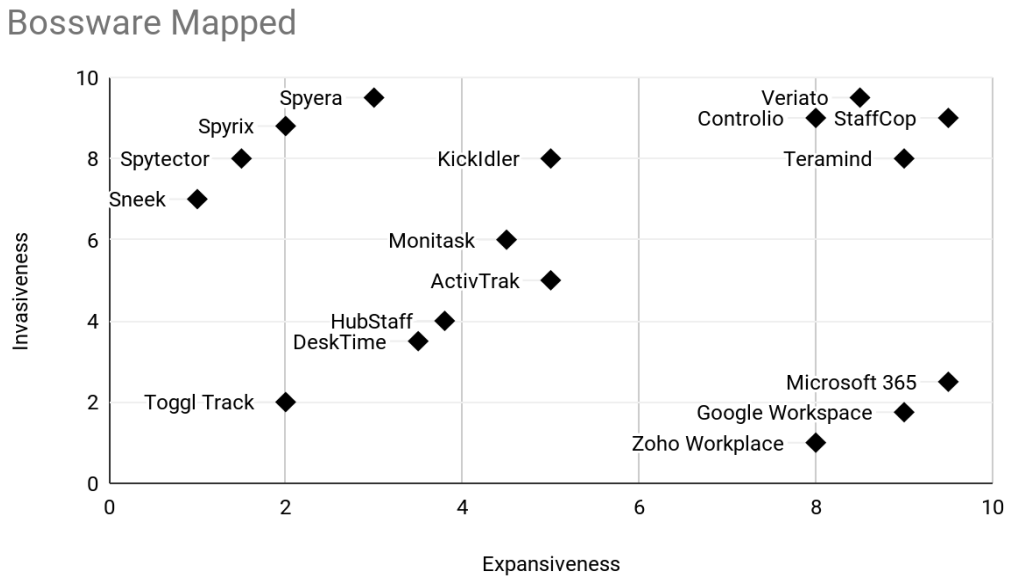

Figure 1: *Mapping employee monitoring software along two axes*

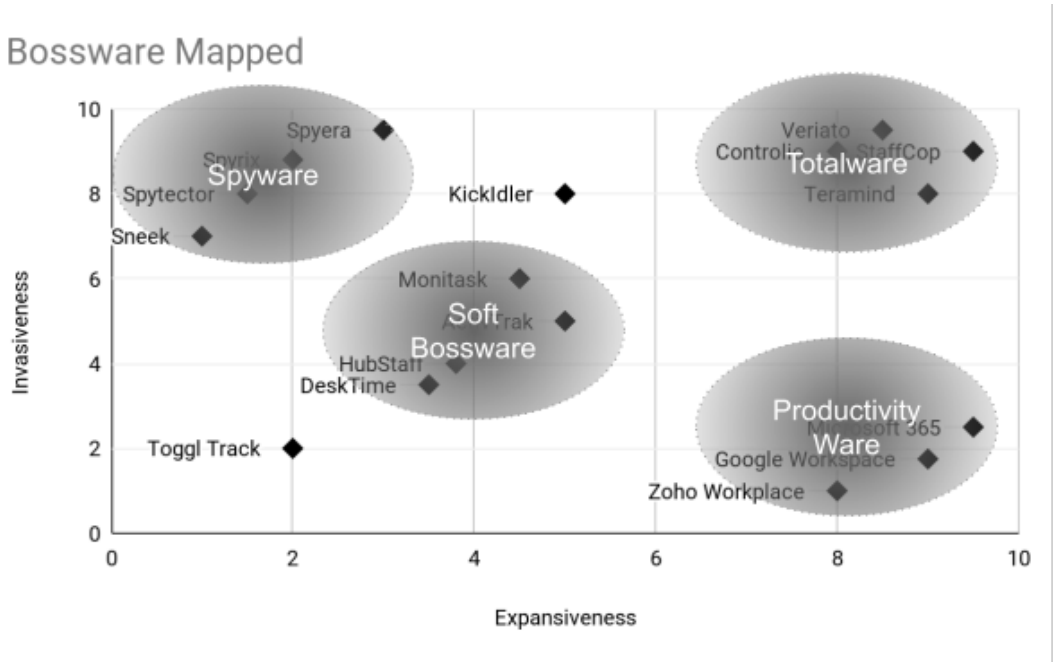

Figure 2: *Provisional bossware typology based on four clusters of points*

Spyware

Spyware in this context refers to the cluster of software in the top left of the chart. These products offer highly revealing forms of surveillance like key logging. In addition, they are typically advertised as using

"stealth mode" by default, deploying these capabilities without any employee knowledge. Such products are unashamedly marketed as a way to digitally eavesdrop on workers undetected, using the language and visual tropes of spying. For this reason, they have high invasiveness scores. However, they also tend to have limited feature-sets, effectively being marketed as "utilities." In addition, these are often older pieces of software that lack the web integration seen in more full-featured suites. For these reasons, they have low expansiveness scores.

Spytector is one product that exemplifies this category. Spytector (2022) markets itself as the ultimate keystroke logger "running in total stealth" and "undetectable even for savvy users." Its website proclaims that it goes undetected by antivirus programs as well. This is highly intrusive and invisible technology. However, key logging is the only feature of this utility. The software was first developed in 2005 to run on older Windows systems. While recent updates have allowed it to run on newer systems, the product still uses a very conventional "shrink-wrapped" licensing model, as opposed to newer cloud-based subscription models or software-as-a-service.

In software terms, spyware is an older form of surveillance, with the bulk of spyware literature, including the most cited articles, dating to a period almost two decades ago (Egele et al. 2007; Good et al. 2005; Kirda et al. 2006). This literature consistently frames spyware as a kind of virus that is installed on users' computers without their knowledge or consent. Such malicious software is often associated with illegitimate activity such as criminals capturing credit card numbers from keyloggers. As a result of this awareness, a range of national and regional anti-spyware legislation was passed at the time (Bowles 2007). Such regulation aimed to hinder the production and distribution of spyware—and these moves arguably contributed to establishing anti-spyware norms. Spyware's age and established notoriety mark it as distinct from the new breed of bossware.

Spyware tends to be highly invasive but also non-expansive, limited in its featureset. Keylogging, as suggested above, can certainly reveal personal details about a user. However, this single data stream is also rather thin and mono-dimensional, collecting keystrokes but not clicks, time on apps, location throughout the day, and so on. If the "goal is to have the most complete picture of the consumer that you can," (Givens 2000: 352), to approximate reality by exhaustively capturing and stitching together datasets (Munn 2017), then this software fails, unable to produce the kind of multifaceted portrait of the worker that is desired.

In addition, spyware tends to be blatant in adopting the language of spying and stealth as its operating model. Such egregious surveillance would seem to place it out of bounds for mainstream companies and larger corporations, limiting its scale and reach. Indeed, companies like Microsoft (2023) specifically include protection mechanisms to identify and remove "spyware and other malicious software." And it's notable that none of these products feature in review roundups on mainstream technology websites (McAllister 2022). Together these points reinforce spyware as an overtly shady product for a niche audience. Spyware is thus notorious but marginal, a combination of factors that should reduce its potential threat to contemporary remote workers.

Totalware

Totalware describes the cluster of software in the upper right of the chart. Products like Controlio and Teramind are full software suites with dozens of modules and features. They offer a highly articulated toolkit to managers and supervisors: smart rules, automated alerts, file transfer auditing, key logging, live screen monitoring, and so on. This broad array of intrusive tools means they score highly on both the invasiveness and expansiveness axes.

The key example here is Teramind. Teramind (2022) is a cloud-based software solution for companies with a vast featureset. Features include live screen capture, remote desktop control, instant message monitoring, online meeting monitoring, and scriptable logics allowing administrators to set up custom rules tied to notifications. The firehose of data that Teramind (2022) collects on each worker can be used to assess

productivity, identify workflow "bottlenecks," and even conduct "forensic" investigations into potential misconduct. Interestingly, this product also contains live OCR recognition, allowing it to decipher words onscreen even when unknown applications are used (Marvin and Sevilla 2020). This expansive and invasive featureset is only tempered slightly by the software presenting administrators with a "visible" and "invisible" option on startup. In both installation and on their website, Teramind (2022) presents the decision to inform employees of monitoring as an important one that requires serious consideration.

Totalware is the strain of bossware that most closely resembles the stereotype of panoptic surveillance. Theorized by Foucault (2020), this schema of open prison cells and a central tower was designed to expose every activity, of every inmate, at every moment. Totalware seeks to replicate this logic of exposure by capturing every keystroke, every message, and every website visit. The goal is to apprehend in meticulous detail the digital footprint of the worker (Manokha 2020). Notably, totalware, with its "invisible" mode, even mirrors the uncertain nature of the panoptic schema. Just as inmates could never be sure if they were being watched, digital workers can never be sure if they are being tracked. The ultimate aim, as with earlier Taylorist forms of surveillance and monitoring, is for workers to internalize the gaze of management (Saval 2014), remaining compliant and productive.

While Foucault's (2020) panopticon was always merely a schema, the combination of contemporary digitally mediated work with sophisticated software makes this vision more attainable. Bossware aims to operationalize this panoptic dream (Manokha 2020; Woodcock 2022)—to monitor an individual's webcam, to log each of their keystrokes, and to track their time down to the second. These exhaustive algorithms and infrastructures keep tabs on every employee throughout the day, "co-constructing the minutiae of work itself—effort, control, performance, and reward" and constitute an intensification of surveillance in the workplace (Ball 2022: 458). Software hopes to realize this fine-grained oversight, turning the theoretical into the computational. However, if this "totalware" certainly constitutes a threat to workers, no technical system is totalizing. As the final section will discuss, intended functionality can be undermined (even if temporarily or partially) by practices of worker resistance.

Soft Bossware

Soft Bossware characterizes the cluster in the center of the chart. This is software that contains many of the standard features of employee monitoring, such as time tracking and screenshotting, but attempts to limit the extent of those features. Monitask, for example, claims to offer "transparency" rather than "spying." It captures the number of keystrokes a user makes but not their content. These products consciously restrict both the invasiveness of their techniques and the expansiveness of the features available to track and monitor. In doing so, they seek to avoid the negative associations of more explicit surveillance. This "bossware-lite" approach promises to deliver insights about productivity without risking a backlash amongst employees.

A prime example of this category is Activtrak. Activtrak (2022) explicitly bills itself as "insight, not oversight" and adopts a conscientious tone, asserting that its software helps assess "productivity and wellness with the employee in mind." Notably for a software company, it frames its lack of features as a benefit: no keystroke logging, no camera access, and no video recording are presented as a positive and more worker-friendly choice, what the company calls the "Activtrak difference." Although the software does track worker practices in many ways, these features are considered to be consistent with the firm's "ethical approach." While such claims should certainly be critiqued (any degree of surveillance presents issues), the focus here is on the more "moderate" featureset, with its tempered invasiveness and expansiveness.

Soft bossware aims to convince companies that its lighter monitoring of workers is appropriate. In other words, it aims to resolve the tension between the employer's surveillance interest and the employee's privacy interest (Watkins-Allen et al. 2007). These companies recognize that workers may have qualms about data being captured, audio being recorded, or "productivity" being tracked—but that these boundaries

are also open to negotiation and modification (Petronio 2002). Granted, all the developers surveyed here rationalize their use of surveillance in some fashion. However, soft bossware backs up these claims with a more tempered feature set. Functionality is designed to provide management oversight while avoiding the critiques associated with invasive surveillance and corporate overreach. This strategy resonates with "soft surveillance" (Marx 2005; Nagenborg 2014), less coercive techniques that are framed as morally ambiguous or even empowering to workers.

In comparison to other bossware types, soft bossware appears as a more subtle kind of threat to workers. Spyware is flagrant in promising to expose individuals through the use of stealth, trickery, and surveillance; similarly, Totalware conforms to popular conceptions of Orwellian or dragnet-style surveillance, totalizing systems that implement exhaustive tracking and monitoring in order to encircle an individual. The "soft bossware" category, by contrast, attempts to walk the tightrope between "acceptable" forms of managerial oversight and "unacceptable" incursions of privacy. And yet this software is still soft surveillance (Marx 2005), capable of tracking web activity, measuring time and "productivity," and sending automated alerts to management based on custom rules. Such software carries out an invasion of privacy, potentially harming a worker's identity, their estimation of themselves, and the image they want to present to others (Alge 2001). Soft bossware is friendlier surveillance, framed in a language of "compliance" and "visibility"—but retaining the core technical operations necessary to identify workers, monitor their workday, and flag anomalous activity.

Productivity Ware

Productivity Ware refers to the cluster of software in the lower right of the chart. This is widely adopted software such as Zoho Workplace and Google Workspace, produced by major technology companies, with user bases in the millions. These suites are highly expansive, incorporating many programs and diverse tools for administrators to gain oversight of workers. However, they lack the most egregious bossware features, they exhibit a higher recognition of privacy and rights, and they wrap safeguards around oversight tools. For this reason, they score much lower on invasiveness.

One product that epitomizes this category is Microsoft 365 (2022). The flagship suite houses a vast array of productivity tools and also integrates with a host of communication, project management, HR, and financial software. This expansive connectivity and its ubiquitous status establishes some powerful surveillance potentials, from the capture of student data (Nemorin 2017) to significant risks around government data (Hildén 2021). However, as a major tech company, Microsoft treads carefully in terms of the features and their optics. After its individual Productivity Score was criticized (Hern 2020), for instance, it was transformed into an Adoption Score that provides aggregate metrics for each company department (Microsoft 365 2022). While such moves are welcome, they are far from being a silver bullet solution to privacy concerns. By using selective queries or combining datasets, supposedly anonymized data can often be de-anonymized (Bampoulidis and Lupu 2019; Sweeney, von Loewenfeldt, and Perry 2018).

As everyday life becomes increasingly carried out via digital technologies, the products that mediate those activities achieve a highly strategic position. Workers schedule appointments, send emails, draft budgets, message colleagues, and collaborate with others through a singular ecosystem. These environments aim to be all-encompassing, providing interoperability between their programs while locking users into their walled garden (Pon, Seppälä, and Kenney 2015). In addition, these suites have extensive user bases. Microsoft 365, for instance, has at least 365 million active users or "paid seats" (Redmond 2022). This is the infrastructure that underpins workers and companies around the world. This tactical combination of massive user bases, multiple "touchpoints" (email, calendars, messaging), and extensive data capture capabilities place productivity ware in a highly strategic position for potential surveillance overreach.

What kinds of data are captured and available within these ubiquitous software environments? Microsoft includes powerful administrative tools in its suite like Audit and Content Search. With the right queries, administrators can read emails, view 1–1 messages in Teams, and see timestamped activities of Office

interactions (Privacy International 2022). Other tech reports have documented how Zoom, Slack, Google, and Microsoft can track user locations, disclose private messages, and reveal scheduled appointments (Surfshark 2022). And yet the surveillance potential of these productivity suites, with the exception of a few passing mentions (Kwet 2019; Nemorin 2017), is almost entirely absent from the literature.

Admittedly, legislative requirements placed on high profile technology companies like Google and Microsoft reign in some of their ability to carry out data extraction, commodification, and monitoring (Buiten 2019; Daskal 2018). However, the rise of bossware also highlights the demand for more monitoring and more fine-grained data over employee practices. Productivity ware would be perfectly placed to carry out this "function creep" (Kuldova 2022) and satisfy this demand if legislation and public sentiment allowed it. For this reason, productivity ware should be understood as a latent risk for workers and its future development closely monitored for signs of incursion and overreach.

Conclusion and Implications

Mainstream press has grasped, not incorrectly, that bossware is something important and potentially dangerous, a new mechanism that significantly shapes contemporary work conditions (Bloomberg 2020; Corbyn 2022; Cyphers and Gullo 2020; Purtill 2022). However, glossing this development as an "Orwellian nightmare" (Drapkin 2022; Settle 2021) flattens the landscape, erasing key distinctions between platforms and products. These distinctions matter: different software has different affordances and different deployments—and all of these factors come together to constitute certain kinds of risks for workers. Such software alters power dynamics in the organization (Miele and Tirabeni 2020) and links data with productivity (Ball 2022) in particular ways. The early mapping above has aimed to offer a more articulated portrait of bossware's diverse landscape.

Bossware, then, is a phenomenon that is both highly dysfunctional and highly powerful. For this reason, further research is urgently needed to better understand the terrain of bossware, its pervasiveness in particular industries, and its psychological and social impacts on workers.

Just as boyd and Crawford (2012) posed a number of critical questions for big data, the mapping carried out here raises a number of critical questions for bossware as an emergent technical phenomenon. It suggests several gaps in knowledge and several possible approaches to interrogating this software, forming an emergent research agenda.

Firstly, employee monitoring software is a corporate product, developed by particular companies for other companies. Software developers for bossware range enormously, from tiny studios to large multinationals. This software development is a social process (Mackenzie 2006) composed of people, tensions, and decisions (Seaver 2022). Each company frames their product in particular ways, rationalizes why it is necessary, and showcases its effectiveness. The legitimacy of this organization and the trust they can foster through this work clearly shapes the uptake of their software product. For example, spyware is developed by niche players for a niche audience, while productivity ware is not even typically viewed as "bossware" and enjoys millions of users in dozens of industries across the globe. Attending to the corporate ecosystem or political economy of this software—the financing, organizational structures, corporate values, and rhetorical legitimacy of its developer and clients—is key for understanding its uptake and application in the world.

Secondly, this software is a technical system. It contains a set of features or affordances, an array of operational capabilities written into code and performed through digital infrastructures. These technical properties significantly alter the processes made available to management, the streams of data that are captured for each worker, and the processing carried out on this data in order to surface patterns and red flags, scores, and metrics. Totalware, for example, brings together a vast array of established software techniques in order to monitor web use, capture audio, track keystrokes, and follow the contemporary worker across the cloud. Software studies (Fuller 2008) and media archeologies (Parikka 2012) are two

approaches that attend closely to these specific technical capacities, their shaping of a technology's use, and their resulting impact on social, cultural, and political life. Opening the black boxes (Pasquale 2015) of these technical systems could contribute to a more articulated understanding of their operations and implications.

Finally, this software exerts a distinct set of work pressures. Here we are focused on the awareness (or suspicion) of workers that their activities are being monitored, the kinds of negotiations and adaptations this requires, and the negative psychosocial impacts of this surveillance, which may include anxiety, stress, mistrust, powerlessness, and alienation (Mendonça et al. 2022). While workplace surveillance is not new, the combination of fine-grained digital tracking with the recent rise of remote work establishes the conditions to intensify these pressures and extend them in new ways. We can estimate the negative fallout on individuals by drawing on older management studies and labor studies (Ball 2010), but how far these findings apply to the new breed of electronic performance monitoring (Ravid et al. 2020) is unclear. For example, recent research suggests that this software's erosion of agency may produce more deviance rather than less (Thiel et al. 2023). Documenting the distinct set of pressures placed on workers by these technical regimes and the precise (and perhaps unexpected) impact this has is a key future task.

The typology constructed above highlights the diversification and expansion of monitoring software in response to demand. There are many companies, with many different product offerings, catering to a wide array of clients. As remote work becomes a significant sphere of labor and work in general becomes more digitally mediated, we would expect this expansion to continue. Telework has already been equated with high imagined surveillance, for example, increasing the expectations that workers place on themselves (Mendonça et al. 2022). Others have suggested that remote workers intentionally seek monitoring and visibility in order for their work to be recognized and remain competitive (Hafermalz 2021). In this sense, employee monitoring leverages the structural precarity of contemporary labor to amplify power asymmetries (Yin 2023), forcing workers to compete against each other, to document their labor, and to prove their worth as employees.

However, along with the intensification and expansion of bossware, we also need to grasp its limitations and modes of resistance. Previous studies on earlier monitoring technologies have shown that workers do not simply acquiesce to this surveillance but resist it by identifying and exploiting weaknesses (Taylor and Bain 1999), distorting captured data to their own advantage (Ferneley, Sobreperez, and Stevens 2004), developing anti-compliant attitudes or resistant intentions to monitoring (Spitzmüller and Stanton 2006), and exchanging complaints and hacks on forums (Ball 2010). These practices of antagonism and obstruction persist in the context of contemporary bossware. In one case, remote workers fought back against activity monitoring by using mouse jigglers and sharing tips for beating the algorithm (Lewis 2021). In another survey, more than half the participants said they would not work for an employer that used remote monitoring (Skillcast 2021).

Whether sabotaging algorithms or refusing to supply their labor altogether, such examples show that bossware is not incontestable. And yet it is also clear that such digital surveillance is a long-term prescription (Maati and Švedkauskas 2021) with highly consequential impacts. Indeed, recent studies suggest data privacy legislation will never sufficiently address workers' needs; new forms of collective governance and worker co-determination must be undertaken to uphold labor rights and foster fair working conditions (Calacci and Stein 2023). Bossware, then, is a key site of power and counterpower in the new terrain of post-pandemic work—and this is what makes it worthy of close attention.

References

Abdullah, Nur Afiqah Akmal, Noor Hanim Rahmat, Fatin Zafirah Zawawi, Muhammad Adib Nazhan Khamsah, and Afiqah Humaira Anuarsham. 2020. Coping with Post COVID-19: Can Work from Home Be a New Norm? *European Journal of Social Sciences Studies* 5 (6): https://oapub.org/soc/index.php/EJSSS/article/view/933/1517.

ActivTrak. 2022. Work Wiser with Workforce Analytics & Productivity Insights. https://www.activtrak.com/ [accessed December 22, 2022].

Ajunwa, Ifeoma. 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.
Alge, Bradley J. 2001. Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice. *Journal of Applied Psychology* 86 (4): 797–804.
Alnumay, Waleed S. 2020. A Brief Study on Software as a Service in Cloud Computing Paradigm. *Journal of Engineering and Applied Sciences* 7 (1): 1–15.
Aloisi, Antonio, and Valerio De Stefano. 2022. Essential Jobs, Remote Work and Digital Surveillance: Addressing the COVID-19 Pandemic Panopticon. *International Labour Review* 161 (2): 289–314.
Apel, Sven, and Christian Kästner. 2009. An Overview of Feature-Oriented Software Development. *The Journal of Object Technology* 8 (5): 1–36.
Armano, Emiliana, Daniela Leonardi, and Annalisa Murgia. 2022. Algorithmic Management in Food Delivery Platforms: Between Digital Neo-Taylorism and Enhanced Subjectivity. *Digital Platforms and Algorithmic Subjectivities* 24: 87–96.
Ball, Kirstie. 2010. Workplace Surveillance: An Overview. *Labor History* 51 (1): 87–106.
———. 2022. Surveillance in the Workplace: Past, Present, and Future. *Surveillance & Society* 20 (4): 455–461.
Bampoulidis, Alexandros, and Mihai Lupu. 2019. An Abstract View on the De-Anonymization Process. arXiv: https://doi.org/10.48550/arXiv.1902.09897.
Barrero, Jose Maria, Nicholas Bloom, and Steven J. Davis. 2020. COVID-19 Is Also a Reallocation Shock. Working Paper, National Bureau of Economic Research. https://doi.org/10.3386/w27137.
Black, Paul W., Thomas O. Meservy, William B. Tayler, and Jeffrey O. Williams. 2022. Surrogation Fundamentals: Measurement and Cognition. *Journal of Management Accounting Research* 34 (1): 9–29.
Bloomberg,. 2020. *How Bossware Is Watching While You Work*. Video. https://www.youtube.com/watch?v=rLjZ6mbodcE [accessed June 9, 2022].
Bowles, L. Elizabeth. 2007. Survey of State Anti-Spyware Legislation. *The Business Lawyer* 63 (1): 301–315.
boyd, danah, and Kate Crawford. 2012. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. *Information, Communication & Society* 15 (5): 662–679.
Buiten, Miriam C. 2019. Regulating Data Giants: Between Competition Law and Data Protection Law. In *New Developments in Competition Law and Economics*, edited by Klaus Mathis and Avishalom Tor, 265–294. Cham, CH: Springer International Publishing.
Calacci, Dan. 2022. Organizing in the End of Employment: Information Sharing, Data Stewardship, and Digital Workerism. In *Proceedngs of the 2022 Symposium on Human-Computer Interaction for Work, Durham, New Hampshire, June 8–9,* 1–9. New York: Association for Computing Machinery.
Calacci, Dan, and Jake Stein. 2023. From Access to Understanding: Collective Data Governance for Workers. *European Labour Law Journal* 14 (2): 253–282.
Campo, Cristina del, Sandra Pauser, Elisabeth Steiner, and Rudolf Vetschera. 2016. Decision Making Styles and the Use of Heuristics in Decision Making. *Journal of Business Economics* 86 (4): 389–412.
Carter, Rebekah. 2021. Understanding Microsoft Productivity Score. *UC Today*, January 15. https://www.uctoday.com/collaboration/understanding-microsoft-productivity-score/ [accessed January 15, 2021].
Corbyn, Zoë. 2022. "Bossware Is Coming for Almost Every Worker": The Software You Might Not Realize Is Watching You. *The Guardian*, April 27. https://www.theguardian.com/technology/2022/apr/27/remote-work-software-home-surveillance-computer-monitoring-pandemic [accessed April 27, 2022].
Coworker. 2021. Bossware and Employment Tech Database. November. https://home.coworker.org/worktech/ [accessed December 19, 2022].
Cyphers, Bennett, and Karen Gullo. 2020. Inside the Invasive, Secretive "Bossware" Tracking Workers. Electronic Frontier Foundation, June 30. https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers [accessed December 19, 2022].
Daskal, Jennifer. 2018. Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0 Essay. *Stanford Law Review Online* 71: 9–16.
De Stefano, Valerio. 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.
Dejours, Christophe, Jean-Philippe Deranty, Emmanuel Renault, and Nicholas H. Smith. 2018. *The Return of Work in Critical Theory: Self, Society, Politics*. New York: Columbia University Press.
Digital.com. 2022. 6 in 10 Employers Require Monitoring Software for Remote Workers. January 31. https://digital.com/6-in-10-employers-require-monitoring-software-for-remote-workers/ [accessed September 6, 2022].
Drapkin, Aaron. 2022. "I Felt Violated… Then Got Used to It"—Employee Monitoring Divides Opinion. *Tech.Co* (blog), February 24. https://tech.co/news/employee-monitoring-software-divides-opinion [accessed December 19, 2022].
Egele, Manuel, Christopher Kruegel, Engin Kirda, Heng Yin, and Dawn Song. 2007. Dynamic Spyware Analysis. In *Proceedings of the Usenix Annual Technical Conference, Santa Clara, California, June 17–22,* 1–14. Berkeley, CA: Advanced Computing Systems Professional and Technical Association.
ExpressVPN. 2021. ExpressVPN Survey Shows Widespread Surveillance on Remote Workers. https://www.expressvpn.com/blog/expressvpn-survey-surveillance-on-the-remote-workforce/ [accessed December 20, 2022].
Ferneley, Elaine, Pauline Sobreperez, and Jason Stevens. 2004. Management Information or Trompe L'Oeil? Resistance to Workplace Surveillance. In *Proceedings of the PACIS 2004, Shanghai, China, July 8–11,* 1000–1009. Atlanta, GA: Association for Information Systems.
Foucault, Michel. 2020. *Discipline and Punish: The Birth of the Prison*. Translated by Alan Sheridan. London: Penguin Books.

Fuller, Matthew. 2008. *Software Studies: A Lexicon.* Cambridge, MA: MIT Press.
Gigerenzer, Gerd, and Wolfgang Gaissmaier. 2011. Heuristic Decision Making. *Annual Review of Psychology* 62: 451–482.
Givens, Beth. 2000. Privacy Expectations in a High Tech World. *Santa Clara High Technology Law Journal* 16 (2): 347–356.
Good, Nathaniel, Rachna Dhamija, Jens Grossklags, David Thaw, Steven Aronowitz, Deirdre Mulligan, and Joseph Konstan. 2005. Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware. In *Proceedings of the 2005 Symposium on Usable Privacy and Security, Pittsburgh, PA, July 6–8,* 43–52. New York: Association for Computing Machinery.
Gregg, Melissa. 2018. *Counterproductive: Time Management in the Knowledge Economy*. Durham, NC: Duke University Press.
Greybeard. 2021. "A Few of My Friends…." Reddit Comment. *R/AskUK*, December 20. www.reddit.com/r/AskUK/comments/pye08x/has_anyone_encountered_bossware_programs_while_at/hetmb8y/.
Hafermalz, Ella. 2021. Out of the Panopticon and into Exile: Visibility and Control in Distributed New Culture Organizations. *Organization Studies* 42 (5): 697–717.
Harwell, Drew. 2020. Managers Turn to Surveillance Software, Always-on Webcams to Ensure Employees Are (Really) Working from Home. *Washington Post*, April 30. https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance/ [accessed December 19, 2022].
Hern, Alex. 2020. Microsoft Productivity Score Feature Criticized as Workplace Surveillance. *The Guardian*, November 26. https://www.theguardian.com/technology/2020/nov/26/microsoft-productivity-score-feature-criticised-workplace-surveillance [accessed December 20, 2022].
Hewitt, Benjamin. 2023. Panoptic Employment: Remote Worker Health Data Under Surveillance. *Science and Technology Law Review* 24 (2): 349–378.
Hildén, Jockum. 2021. Mitigating the Risk of US Surveillance for Public Sector Services in the Cloud. *Internet Policy Review* 10 (3): 1–24.
Holman, David, Claire Chissick, and Peter Totterdell. 2002. The Effects of Performance Monitoring on Emotional Labor and Well-Being in Call Centers. *Motivation and Emotion* 26 (1): 57–81.
Hunter, Tatum. 2021. Here Are All the Ways Your Boss Can Legally Monitor You. *Washington Post*, October 4. https://www.washingtonpost.com/technology/2021/08/20/work-from-home-computer-monitoring/ [accessed December 20, 2022].
iMonitor. 2022. Employee Monitoring Software. https://www.imonitorsoft.com/ [accessed December 19, 2022].
IndustryARC. 2021. Employee Monitoring Software Market Research Report. https://www.industryarc.com/Report/19332/employee-monitoring-software-market.html [accessed December 20, 2022].
Katsabian, Tammy. 2020. The Telework Virus: How the COVID-19 Pandemic Has Affected Telework and Exposed Its Implications for Privacy and Equality. SSRN, September 1. https://doi.org/10.2139/ssrn.3684702.
Kennedy, Russell. 2018. Enhancing the Workplace or an Intrusion of Privacy? As Surveillance Technology Continues to Evolve, so Too Will the Debate. September 4. 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 [accessed May 9, 2024].
Kirda, Engin, Christopher Kruegel, Greg Banks, Giovanni Vigna, and Richard Kemmerer. 2006. Behavior-Based Spyware Detection. In *Proceedings of the Usenix Security Symposium, Vancourver, CA, July 31–August 4*, 273–288. Berkeley, CA: The Advanced Computing Systems Association.
Klein, Naomi. 2007. *The Shock Doctrine: The Rise of Disaster Capitalism*. New York: Macmillan.
Klosowski, Thorin. 2022. There's (Probably) Nothing You Can Do About the New Bossware That's Spying on You. *Wirecutter: Reviews for the Real World* (blog), June 6. https://www.nytimes.com/wirecutter/blog/what-to-do-about-bossware-employee-monitoring/ [accessed December 19, 2022].
Kuldova, Tereza Østbø. 2022. Artificial Intelligence, Algorithmic Governance, and the Manufacturing of Suspicion and Risk. In *Compliance-Industrial Complex: The Operating System of a Pre-Crime Society*, edited by Tereza Østbø Kuldova, 115–151. Cham, CH: Springer Nature Switzerland.
Kwet, Michael. 2019. Digital Colonialism: US Empire and the New Imperialism in the Global South. *Race & Class* 60 (4): 3–26.
Lasprogata, Gail, Nancy King, and Sukanya Pillay. 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.
Lewis, Norman. 2021. Remote Workers Find Ways to Trick 'Bossware' Spying. RT International, December 11. https://www.rt.com/op-ed/542905-bossware-spying-mouse-mover/ [accessed September 6, 2022].
Light, Ben, Jean Burgess, and Stefanie Duguay. 2018. The Walkthrough Method: An Approach to the Study of Apps. *New Media & Society* 20 (3): 881–900.
Liu, Hong Yu. 2022. Digital Taylorism in China's e-Commerce Industry: A Case Study of Internet Professionals. *Economic and Industrial Democracy* 44 (1): 1–18.
Lloyd, Anthony. 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.
Lomborg, Stine. 2022. Everyday AI at Work: Self-Tracking and Automated Communication for Smart Work. In *Everyday Automation*, edited by Sarah Pink, Martin Berg, Deborah Lupton, and Minna Ruckenstein, 126–39. London: Routledge.
Lyon, David. 2021. *Pandemic Surveillance*. London: Wiley.
Ma, Dan. 2007. The Business Model of "Software-As-A-Service." In *IEEE International Conference on Services Computing, Salt Lake City, Utah, July 9–13,* 701–702.
Maati, Ahmed, and Žilvinas Švedkauskas. 2021. Long-Term Prescription? Digital Surveillance Is Here to Stay. *Czech Journal of International Relations* 56 (4): 105–118.
MacKenzie, Adrian. 2006. *Cutting Code: Software and Sociality*. New York: Peter Lang.
Macnish, Kevin. 2015. An Eye for an Eye: Proportionality and Surveillance. *Ethical Theory and Moral Practice* 18: 529–548.

Manley, Andrew, and Shaun Williams. 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.
Manokha, Ivan. 2020. The Implications of Digital Employee Monitoring and People Analytics for Power Relations in the Workplace. *Surveillance and Society* 18 (4): 540–554.
Marvin, Rob, and Gadjo Sevilla. 2020. Teramind Review. *PC Magazine*, October 1. https://au.pcmag.com/cloud-services-1/50572/teramind [accessed December 20, 2022].
Marx, Gary. 2004. Some Concepts That May Be Useful in Understanding the Myriad Forms and Contexts of Surveillance. *Intelligence & National Security* 19 (2): 226–248.
———. 2005. Soft Surveillance: Mandatory Voluntarism and the Collection of Personal Data. *Dissent* 52 (4): 36–43.
Marx, Karl. 1977 [1867]. *Capital: A Critique of Political Economy*. Translated by Ben Fowkes. London: Vintage.
Mcallister, Neil. 2022. The Best Employee Monitoring Software for 2023. *PCMag Australia*, January 20. https://au.pcmag.com/cloud-services-1/50574/the-best-employee-monitoring-software [accessed March 7, 2023].
Mendonça, Inês, Franz Coelho, Paulo Ferrajão, and Ana Maria Abreu. 2022. Telework and Mental Health during COVID-19. *International Journal of Environmental Research and Public Health* 19 (5): https://doi.org/10.3390/ijerph19052602.
Microsoft. 2023. Malware and Ransomware Protection in Microsoft 365—Microsoft Service Assurance. March 2. https://learn.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection [accessed March 7, 2023].
Microsoft 365. 2022. Microsoft Adoption Score. February 12. https://learn.microsoft.com/en-us/microsoft-365/admin/adoption/adoption-score [accessed December 20, 2022].
Miele, Francesco, and Lia Tirabeni. 2020. Digital Technologies and Power Dynamics in the Organization: A Conceptual Review of Remote Working and Wearable Technologies at Work. *Sociology Compass* 14 (6): https://doi.org/10.1111/soc4.12795.
Migliano, Simon. 2022. Employee Monitoring Software Demand Trends 2020–22. Top10VPN, November 9. https://www.top10vpn.com/research/covid-employee-surveillance/ [accessed December 19, 2022].
Milmo, Dan. 2021. Algorithmic Tracking Is "Damaging Mental Health" of UK Workers." *The Guardian*, November 11. https://www.theguardian.com/technology/2021/nov/11/algorithmic-monitoring-mental-health-uk-employees [accessed December 22, 2022].
Moses, Lyria Bennett. 2007. Recurring Dilemmas: The Law's Race to Keep up with Technological Change. University of Illinois Journal of Law, Technology, & Policy 7: 239–285.
Munn, Luke. 2017. Seeing With Software: Palantir and the Regulation of Life. *Studies In Control Societies* 2 (1): https://studiesincontrolsocieties.org/seeing-with-software/.
———. 2022. *Automation Is a Myth*. Stanford, CT: Stanford University Press.
Nagenborg, Michael. 2014. Surveillance and Persuasion. *Ethics and Information Technology* 16 (1): 43–49.
Nemorin, Selena. 2017. Post-Panoptic Pedagogies: The Changing Nature of School Surveillance in the Digital Age. *Surveillance & Society* 15 (2): 239–253.
Nott, George. 2018. Legally Snooping on Employees a Doddle in Australia, Finds Law Firm Analysis." CIO, February 19. https://www.cio.com/article/213583/legally-snooping-on-employees-a-doddle-in-australia-finds-law-firm-analysis.html [accessed October 28, 2022].
O'Neill, Christopher. 2017. Taylorism, the European Science of Work, and the Quantified Self at Work. *Science, Technology, & Human Values* 42 (4): 600–621.
Parikka, Jussi. 2012. *What Is Media Archaeology?* London: Polity.
Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.
Petronio, Sandra. 2002. *Boundaries of Privacy:Dialectics of Disclosure.* Albany, NY: SUNY Press.
Pon, Bryan, Timo Seppälä, and Martin Kenney. 2015. One Ring to Unite Them All: Convergence, the Smartphone, and the Cloud. *Journal of Industry, Competition and Trade* 15 (1): 21–33.
Privacy International. 2022. WFH—Watched from Home: Office 365 and Workplace Surveillance Creep. Privacy International. June 15. http://privacyinternational.org/long-read/4909/wfh-watched-home-office-365-and-workplace-surveillance-creep [accessed March 9, 2023].
Purtill, James. 2022. Employers Using Software Monitoring Is Now the New Norm. Here's How Some Workers Get around It. *ABC News*, May 5. https://www.abc.net.au/news/science/2022-05-06/workers-returning-to-offices-covid-surveillance-software/101019128 [accessed December 20, 2022].
Ravid, Daniel M, David L Tomczak, Jerod C White, and Tara S Behrend. 2020. EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring. *Journal of Management* 46 (1): 100–126.
Redmond, Tony. 2022. Office 365 Number of Users Reaches 345 Million Paid Seats. April 28. https://office365itpros.com/2022/04/28/office-365-number-of-users/ [accessed March 7, 2023].
Ridgway, V. F. 1956. Dysfunctional Consequences of Performance Measurements. *Administrative Science Quarterly* 1 (2): 240–247.
Sandberg, Ake. 1994. "Volvoism" at the End of the Road? *Studies in Political Economy* 45 (1): 170–182.
Saval, Nikil. 2014. *Cubed: A Secret History of the Workplace*. New York: Doubleday.
Schooley, Skye. 2022. Best Employee Monitoring Software Platforms. *Business News Daily*, December 15. https://www.businessnewsdaily.com/11143-best-employee-monitoring-software.html [accessed December 21, 2022].
Seaver, Nick. 2022. *Computing Taste: Algorithms and the Makers of Music Recommendation*. Chicago, IL: University of Chicago Press.

Settle, Mark. 2021. The Digitally Transformed Workplace: Productivity Paradise Or Orwellian Nightmare? *Forbes*, September 14. https://www.forbes.com/sites/marksettle/2021/09/14/the-digitally-transformed-workplace-productivity-paradise-or-orwellian-nightmare/ [accessed December 19, 2022].

Skillcast. 2021. Remote-Worker Monitoring YouGov Survey. London: March 21. https://www.skillcast.com/blog/remote-worker-monitoring-yougov-survey [accessed December 21, 2021].

Soares, Sergei, Florence Bonnet, and Janine Berg. 2021. Working from Home during the COVID-19 Pandemic: Updating Global Estimates Using Household Survey Data. VoxEU.Org (blog), April 25. https://voxeu.org/article/working-home-during-covid-19-pandemic-updated-estimates [accessed March 7, 2023].

Spitzmüller, Christiane, and Jeffrey M. Stanton. 2006. Examining Employee Compliance with Organizational Surveillance and Monitoring. *Journal of Occupational and Organizational Psychology* 79 (2): 245–272.

Sprague, Robert. 2007. From Taylorism to the Omnipticon: Expanding Employee Surveillance beyond the Workplace. *Journal of Computer & Information Law* 25 (1): 1–35.

Spytector. 2022. Spytector—Undetectable KeyLogger for 32-Bit and 64-Bit Windows OS. December 1. https://www.spytector.com [accessed December 20, 2022].

Stegman, Jonah, Patrick J Trottier, Caroline Hillier, Hassan Khan, and Mohammad Mannan. 2022. "My Privacy for Their Security": Employees' Privacy Perspectives and Expectations When Using Enterprise Security Software. *ArXiv Preprint*. https://www.usenix.org/system/files/sec23summer_301-stegman-prepub.pdf.

Surfshark. 2022. Employee Surveillance Report. https://surfshark.com/employee-surveillance [accessed December 20, 2022].

Sweeney, Latanya, Michael von Loewenfeldt, and Melissa Perry. 2018. Saying It's Anonymous Doesn't Make It So: Re-Identifications of "Anonymized" Law School Data. *Technology Science*, November 12. https://techscience.org/a/2018111301/ [accessed March 15, 2023].

Taylor, Frederick Winslow. 1913. *The Principles of Scientific Management*. New York: Harper.

Taylor, Phil, and Peter Bain. 1999. "An Assembly Line in the Head": Work and Employee Relations in the Call Centre. *Industrial Relations Journal* 30 (2): 101–117.

Teramind. 2022. Insider Threat Detection & Employee Monitoring. https://www.teramind.co [accessed December 22, 2022].

Thiel, Chase E., Julena Bonner, John T. Bush, David T. Welsh, and Niharika Garud. 2023. Stripped of Agency: The Paradoxical Effect of Employee Monitoring on Deviance. *Journal of Management* 49 (2): 709–740.

Watkins-Allen, Myria, Stephanie J. Coopman, Joy L. Hart, and Kasey L. Walker. 2007. Workplace Surveillance and Managing Privacy Boundaries. *Management Communication Quarterly* 21 (2): 172–200.

White, Marilyn Domas, and Emily E. Marsh. 2006. Content Analysis: A Flexible Methodology. *Library Trends* 55 (1): 22–45.

Williamson, Sue, Linda Colley, and Sally Hanna-Osborne. 2020. Will Working from Home Become the "New Normal" in the Public Sector? *Australian Journal of Public Administration* 79 (4): 601–607.

Woodcock, Jamie. 2022. The Algorithmic Panopticon at Deliveroo: Measurement, Precarity, and the Illusion of Control. *Ephemeral Journal* 22 (2): https://ephemerajournal.org/contribution/algorithmic-panopticon-deliveroo-measurement-precarity-and-illusion-control-0.

WordSense. 2022. Bossware. WordSense Dictionary. https://www.wordsense.eu/bossware/ [accessed December 20, 2022].

Yin, Siyuan. 2023. Situating Platform Gig Economy in the Formal Subsumption of Reproductive Labor: Transnational Migrant Domestic Workers and the Continuum of Exploitation and Precarity. *Capital & Class* 48 (1): https://doi.org/10.1177/03098168221145407.

Zubicki, Monique. 2022. The Myths and Truths of Employee Monitoring. Veriato, October 20. https://veriato.com/blog/myths-truths-employee-monitoring/ [accessed March 7, 2023].