LIVERPOOL
JOHN MOORES
UNIVERSITY

LJMU Research Online

**Kayas, OG, Ong, CE and Belal, HM**

**From humans to algorithms: A sociotechnical framework of workplace surveillance**

**https://researchonline.ljmu.ac.uk/id/eprint/26199/**

**Article**

**Citation** (please note it is advisable to refer to the publisher's version if you intend to cite from this work)

**Kayas, OG, Ong, CE and Belal, HM (2025) From humans to algorithms: A sociotechnical framework of workplace surveillance. Digital Business, 5 (2). ISSN 2666-9544**

LJMU has developed **LJMU Research Online** for users to access the research output of the University more effectively. Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Users may download and/or print one copy of any article(s) in LJMU Research Online to facilitate their private study or for non-commercial research. You may not engage in further distribution of the material or use it for any profit-making activities or any commercial gain.

The version presented here may differ from the published version or from the version of the record. Please see the repository URL above for details on accessing the published version and note that access may require a subscription.

For more information please contact researchonline@ljmu.ac.uk

http://researchonline.ljmu.ac.uk/

Digital Business 5 (2025) 100120

Contents lists available at ScienceDirect

Digital Business

journal homepage: www.elsevier.com/locate/digbus

# From humans to algorithms: A sociotechnical framework of workplace surveillance

Oliver G. Kayas [b,*], Chin Eang Ong [a,b], H.M. Belal [a,b]

[a] *Liverpool Business School, United Kingdom*
[b] *Liverpool John Moores University, Student Life Building, 10 Copperas Hill, Liverpool L3 5AH, United Kingdom*

ARTICLE INFO

*Keywords:*
Digital technology
Sociotechnical
Surveillance
Algorithm
Resistance

ABSTRACT

Workplace surveillance is a sociotechnical practice shaped by both human actors and digital technology. Although existing surveillance frameworks acknowledge the role that social context plays in shaping the outcomes of surveillance, they overlook the impact organisational culture, leadership, management, and employees have on shaping its characteristics. Current frameworks also underplay the influence of digital technology and fail to account for the impact modern digital technologies, such as artificial intelligence algorithms, have on shaping the characteristics of surveillance. Through an inductive approach that synthesises and integrates surveillance concepts and theories, this paper identifies and develops the characteristics of surveillance (i.e., purpose, observer, target, direction, transparency, and intrusiveness) as well as the specific social and technological elements shaping each characteristic. By integrating these dimensions, this paper produces an innovative sociotechnical framework that provides academics and practitioners with a detailed understanding of the various types of surveillance engendered in different organisational settings. This paper also sheds light on how the social and technological elements interact to shape the characteristics of surveillance, the negative outcomes and ethical challenges arising from each characteristic, and approaches to mitigating these negative effects. In addition, practical recommendations are offered to guide organisations with the responsible implementation of surveillance through a participatory process aligned with organisational policies and legal and regulatory requirements. These practical recommendations can also help organisations reduce resistance, improve trust between employers and employees, mitigate negative outcomes, avoid ethical concerns, and increase acceptance of surveillance.

## 1. Introduction

With the advent of the COVID-19 pandemic and the subsequent increase in the number of people working remotely, employees have found themselves subjected to an increasing sarray of surveillance practices underpinned by digital technology (Mettler, 2023), including artificial intelligence (AI), machine learning algorithms, body implants, biometric devices, sensors, social networks, and workplace analytics. Amazon, for example, captures every minute of workers' *time off task* (e.g., time spent in the bathroom or talking to colleagues) using radio frequency handheld scanners, with those who exceed 30 minutes on three separate days being fired for breaching thresholds (Parkes, 2023). Employers also use laptop monitoring software to take snapshots of employee screens and provide performance scores that measure computer activity. Elsewhere, construction workers have been forced to use biometric sign-ins and GPS tracking apps to monitor their productivity (Big Brother Watch, 2024). Through the collection of increasingly personal and sensitive data that may not be related to work, such as employees' beliefs, likes, emotions, wellness, fitness, and health, digital technologies provide employers with the ability to compare sensed information with predefined standards and thresholds to determine whether they have achieved organisational expectations (Ball, 2021; Mettler, 2023; Seppänen et al., 2025).

Although digital technologies can extend employers' surveillance capabilities, social actors within an organisation's particular social context play a vital role in shaping the development and use of surveillance practices. Indeed, Lyon (2003) argues that the interconnectedness between the social and technological dimensions of surveillance practices are used to manage populations. He purports that while computers sort out transactions, interactions, visits, calls, and other

[*] Corresponding author at: Liverpool John Moores University, Student Life Building, 10 Copperas Hill, Liverpool L3 5AH, United Kingdom.
*E-mail addresses:* o.g.kayas@ljmu.ac.uk (O.G. Kayas), c.e.ong@ljmu.ac.uk (C.E. Ong), h.m.belal@ljmu.ac.uk (H.M. Belal).

https://doi.org/10.1016/j.digbus.2025.100120
Received 16 January 2025; Received in revised form 18 March 2025; Accepted 6 April 2025
Available online 9 April 2025
2666-9544/© 2025 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

activities to permit or deny access to events, experiences, and processes, "socio-technical surveillance systems are also affected by people complying with, negotiating, or resisting surveillance" (Lyon, 2003, p. 14).

In the narrower context of the workplace, Ball's (2002) surveillance framework argues that the social and technological dimensions of surveillance comprise four elements, perpetuated through interactions between technology and people: *representation*, relating to the material aspects of a person captured and inscribed by technology; *meaning*, referring to the socially constructed interpretation of data about those subjected to surveillance; *manipulation*, referring to how elements of surveillance regulate and configure power relations; and *intermediation*, referring to how surveillance is sustained. The psychology-focused typology by Ravid et al. (2020) provides a set of foundational characteristics related to the purpose, invasiveness, synchronicity, and transparency of electronic performance monitoring. Incorporating the attitudinal and motivational effects of performance monitoring, Stanton's (2000) framework examines employee responses to monitoring, highlighting its impact on performance appraisals and feedback. Ball and Margulis's (2011) framework examines the social processes surrounding monitored employee tasks in call centres. The model of industrial labour process control by Sewell (1998) analyses how electronic surveillance interacts with peer-group scrutiny, while Sewell and Barker (2006) develop two competing forms of workplace surveillance, acknowledging the ambiguity and paradox between its *coercive* and *caring* aspects. Building on this work, Sewell et al. (2011) identify three elements of analysis (legitimacy, purpose, and evaluation) underpinning a conceptualisation of surveillance that moves beyond the decision between performance measurement as a form of care or coercion.

Despite their valuable contributions, these frameworks tend to focus on the outcomes of workplace surveillance, rather than how the social and technological dimensions shape the characteristics of surveillance in different organisations, including its purpose, who observes (humans or machines), who is targeted, its direction (vertical or horizontal), the degree to which targets are informed about surveillance (transparency), and its level of intrusiveness. Indeed, existing surveillance frameworks focus on explaining how social actors and social context influence the outcomes of surveillance while largely neglecting the role of digital technology (i.e., Ball & Margulis, 2011; Ravid et al., 2020; Sewell, 1998; Sewell et al., 2011; Sewell & Barker, 2006; Stanton, 2000). Existing frameworks also focus on explaining how social context shapes the characteristics of surveillance while underplaying or overlooking the role of digital technology (i.e., Ball & Margulis, 2011; Ravid et al., 2020; Sewell, 1998; Sewell et al., 2011; Sewell & Barker, 2006; Stanton, 2000). Moreover, despite empirical studies revealing the significant impact organisational culture, leadership, management, and employees have on shaping the characteristics of surveillance (e.g., Alder, 2001; de Vries & van Gelder, 2015; Hafermalz, 2021), they have not been integrated within previous surveillance frameworks (i.e., Ball, 2002; Ball & Margulis, 2011; Ravid et al., 2020; Sewell, 1998; Sewell et al., 2011; Sewell & Barker, 2006; Stanton, 2000).

Furthermore, previous frameworks are yet to explore the impact new digital technology has on the sociotechnical conditions shaping the characteristics of workplace surveillance (i.e., Ball, 2002; Ball & Margulis, 2011; Ravid et al., 2020; Stanton, 2000). Surveillance practices using machine learning algorithms, for example, have removed humans from the loop by automating surveillance processes (Kayas, 2024; Newlands, 2021). In addition, despite multiple calls (Ball, 2021; Ball & Margulis, 2011; Kayas, 2023; Ravid et al., 2020), existing frameworks treat leaders and managers as observers and employees as monitored subjects (i.e., Ball, 2002; Ball & Margulis, 2011; Ravid et al., 2020; Sewell, 1998; Sewell et al., 2011; Sewell & Barker, 2006; Stanton, 2000), while failing to consider empirical research showing that they too are actors targeted by surveillance (e.g., Bush et al., 2010; Cabral & Lazzarini, 2015; Chen, 2016; Kayas, 2023; Xiang, 2020). Previous frameworks also focus on the impact that surveillance has on employees, rather than considering their influence on shaping the characteristics of surveillance alongside leaders and managers.

Against this backdrop, this paper aims to produce a sociotechnical framework to explain how the social and technological dimensions within an organisation shape the characteristics of workplace surveillance. Through a conceptual research approach, this paper thus identifies and develops the characteristics of surveillance as well as the social and technological elements shaping each characteristic. As a result, this paper produces a comprehensive sociotechnical framework that provides academics and practitioners with a detailed understanding of the various characteristics of surveillance engendered in different organisational settings. It also reveals how the social and technological elements within an organisation interact to shape the characteristics of surveillance, the negative outcomes and ethical challenges arising from each characteristic, and approaches to mitigating these negative effects. In addition, this paper proposes practical recommendations to guide organisations with the responsible implementation of surveillance through a participatory process aligned with organisational policies and legal and regulatory requirements. These practical recommendations can help organisations reduce resistance, improve trust between employers and employees, mitigate negative outcomes, avoid ethical concerns, and increase acceptance of surveillance.

This paper proceeds by providing an overview of workplace surveillance. It then develops the elements of the social and technological dimensions shaping workplace surveillance. The paper then develops the characteristics of workplace surveillance and discusses how each of the social and technological elements shape each characteristic. Practical recommendations are then proposed for organisations, leaders, managers, employees, and policy makers. The paper concludes by outlining the paper's contributions, limitations, and opportunities for future research.

## 2. Workplace surveillance

The word surveillance, borrowed from French to English in the 19th century, literally means to *watch over* (*sur* 'over' and *veiller* 'watch'), both of which come from Latin, *vigilare*, to keep watch. In this sense, surveillance is an everyday practice in which humans routinely engage, often without thinking about it (Lyon, 2001). It could be a parent watching their child, a lifeguard watching swimmers, a doctor watching patients, or a manager watching employees. Jeremy Bentham's (1791) early theoretical treatment of surveillance led to the development of the panopticon. An architectural apparatus designed to control people's behaviour through observations made by unseen human observers. The principal idea is that the power dynamic between the observer and the observed encourages self-discipline among those observed because of a fear of disciplinary punishment. Foucault (1977) later extended the panopticon as a metaphor for the disciplinary power and surveillance that permeate the institutions in a society.

In recent decades, the practice of surveillance has transformed as human-orientated approaches to surveillance have been imbricated with electronic mediation (Kayas, 2023). This prompted Zuboff (1988) to develop the information panopticon, which uses electronic systems (not humans) to automatically capture information about surveillance targets. The advancement of digital technologies, such as AI algorithms, has driven new theoretical developments, including surveillance capitalism. It involves the mechanisms of data extraction, commodification, and control exiling subjects from their own behaviour through behavioural prediction and modification (Zuboff, 2015). As a result of these digital transformations, surveillance has been defined as "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" (Lyon, 2001, p. 2). This definition underscores how the digital technology underpinning the technocentric activity of surveillance involves social actors and has social implications (Ball, 2002).

In the narrower context of the workplace, organisational processes have been augmented with electronic mediation since the 1980s, enabling employers to monitor employees in real-time across public-private boundaries as well as outside traditional organisational boundaries (Ball, 2021; Kayas, 2023; Ravid et al., 2020). Based on the Office of Technology Assessment (1987) model (Fig. 1), Ball (2010, p. 87) defines workplace surveillance as "management's ability to monitor, record and track employee performance, behaviours and personal characteristics in real-time (for example, Internet or telephone monitoring) or as part of broader organizational processes (for example, drug testing in recruitment)." This widely accepted definition implies a top-down approach to surveillance, with leaders and managers using technology to monitor employees, despite empirical research showing that leaders and managers are also subjected to surveillance (Ball & Margulis, 2011; Kayas, 2023). Indeed, organisations use digital technology to monitor the behaviour, performance, and personal characteristics of employees, leaders, and managers to assess whether strategic objectives are achieved, identify illegitimate insider trading, and confirm whether expenses are accurately reported (Chen, 2016). Organisations also implement surveillance systems to determine whether managers comply with ethical policies (Bush et al., 2010), prevent bribery and shirking (Xiang, 2020), and evaluate performance (Kayas et al., 2019).

However, workplace surveillance can cause significant negative outcomes for leaders, managers, and employees. It can heighten the anxiety and stress of employees engaged in tasks that are monitored and judged against strict performance targets (Schleifer & Shell, 1992; Smith et al., 1992). It can engender unethical behaviours among leaders and managers who find monitoring a frustrating and time-consuming issue, detracting from other valuable uses of their time (Bush et al., 2010). Subjecting employees to intrusive surveillance practices has even been shown to lower job satisfaction, commitment, and morale (Chalykoff & Kochan, 1989; Charbonneau & Doberstein, 2020; da Cunha et al., 2015). In the case of algorithmic surveillance, it can erode employees' autonomy by transferring their decision-making responsibilities to algorithmic technologies (Levy, 2015). Furthermore, if the propensity to trust is low because employees are perceived as underperforming, shirking, loafing, or misbehaving, then leaders are more likely to intensely monitor employees (Alge et al., 2004; De Jong & Elfring, 2010; Sewell, 1998). This erodes trust between employees and employers, which can in turn undermine performance, encourage unethical behaviours, increase the likelihood of resistance, and lower perceptions of fairness (Bush et al., 2010; De Jong & Elfring, 2010; Kayas et al., 2019; Westin, 1992). To mitigate against a reduction in trust, leaders and managers should develop interpersonal relationships that help foster trust between themselves and employees (De Jong & Elfring, 2010).

Workplace surveillance also raises serious ethical concerns about privacy, consent, and security. Although employers have a right to monitor employee performance and behaviour (Kayas, 2023), this threatens their right to privacy (Bhave et al., 2019). Hidden surveillance technologies, such as Google Glass, for example, can infringe on employees' privacy and security if customers take photos of them without their consent (Ball, 2016). To gain employment, Amazon drivers must sign a consent form so that the surveillance system in the delivery truck can access their location, movement, and biometric data (Gurley, 2022). Ravid et al. (2020) outline how electronic surveillance practices raise privacy and security concerns by capturing behavioural data about the internal states and private behaviours of individuals without warning or consent. Given the contested legal terrain and the lack of regulation (Ball, 2021), it is unsurprising that privacy, consent, and security are of growing concern.

These negative outcomes and ethical concerns increase the likelihood of employees retaliating through acts of resistance (Ball, 2021). Despite organisational attempts to ensure employees conform to the behaviours leaders and managers embed within surveillance, there are always blind spots or technology-mediated gaps where employees can resist (Ball, 2010; Sewell, 1998; Sewell et al., 2011). Employees can adopt various strategies in their struggle against surveillance, including rule-bending, strikes, working to rules, and withdrawal of cooperation (Woodcock, 2021). Employees also resist through organisational misbehaviour strategies, including acts of sabotage, theft, vandalism, time-wasting, and humour directed against employers, leaders, and managers (Kayas, 2023). While employers perceive such acts of resistance as counterproductive irritants that can freeze an organisation into disfunction, activists argue that they are a necessary response to forms of organisational power and domination embedded in surveillance.

## 3. Methodology

This study adopted a conceptual research approach to develop the sociotechnical framework of workplace surveillance (Jaakkola, 2020). Unlike empirical studies that collect and analyse primary data, arguments were derived through the synthesis and integration of evidence rooted in previously developed surveillance concepts and theories (Hirschheim, 2008). This supported the construction of a sociotechnical framework of surveillance that bridges existing theories and concepts across disciplines, produces new and deeper multilevel insights, and provides a broader scope of thinking (Gilson & Goldberg, 2015).

To develop the framework, an inductive approach was followed, deriving theoretical insights from research in the literature (Jaakkola, 2020). Therefore, existing studies on workplace surveillance, digital technology, and information systems were analysed to inform the

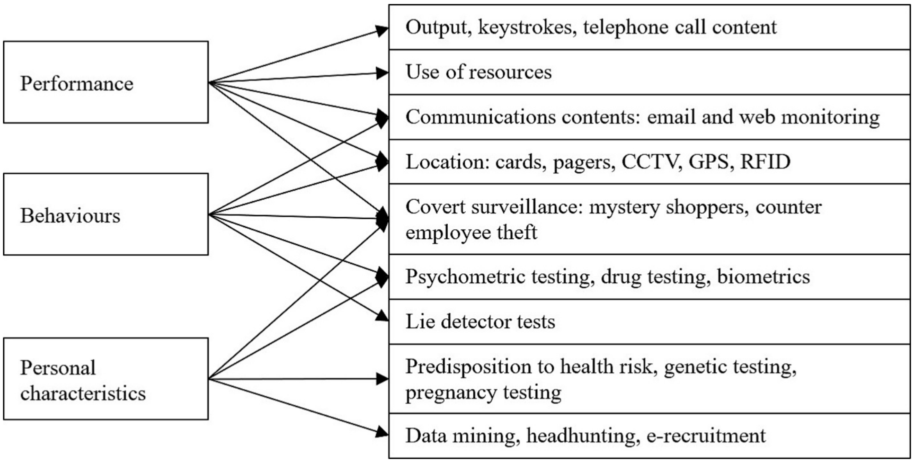

Performance
Behaviours
Personal characteristics
Output, keystrokes, telephone call content
Use of resources
Communications contents: email and web monitoring
Location: cards, pagers, CCTV, GPS, RFID
Covert surveillance: mystery shoppers, counter employee theft
Psychometric testing, drug testing, biometrics
Lie detector tests
Predisposition to health risk, genetic testing, pregnancy testing
Data mining, headhunting, e-recruitment

**Fig. 1.** Surveillance practices used to monitor employees.
*Source:* Ball (2010).

development of the elements shaping the social and technological dimensions of surveillance as well as the characteristics of surveillance (Jaakkola, 2020). Empirical findings from the literature were used as secondary sources to elucidate the different ways in which surveillance manifests itself in various organisational settings (Hirschheim, 2008; Jaakkola, 2020). The sociotechnical framework was constructed by systematically categorising the elements that shape workplace surveillance into two dimensions: the social dimension (i.e., organisational culture, leadership, management, and employees) and the technological dimension (i.e., focus, boundary, datafication, automation, timeline, and frequency). Each of these elements was then mapped against the characteristics of surveillance (i.e., purpose, observer, target, direction, transparency, and intrusiveness) to illustrate how both the social and technological dimensions shape surveillance outcomes. This process allowed for the development of a structured but flexible conceptualisation of workplace surveillance, ensuring both theoretical rigour and real-world relevance (Gilson & Goldberg, 2015; Hirschheim, 2008).

## 4. A sociotechnical framework of workplace surveillance

To create the sociotechnical framework, this section develops the specific elements of the social and technological dimensions that shape the characteristics of workplace surveillance.

### *4.1. The social dimension*

Social actors within an organisation's particular social context influence the characteristics of the surveillance deployed (Ball, 2010; Kayas, 2023). Indeed, 'actors do not behave or decide as atoms outside a social context' (Granovetter, 1985, p. 487); rather, they make sense of their organisation by creating meanings based on ideas rooted in their immediate environment, as well as the broader institutional environments pertaining to social systems within and around their work and organisation (Ball & Margulis, 2011). Despite empirical studies showing the significant impact surveillance practices have on organisational culture, leadership, management, and employees (e.g., Alder, 2001; de Vries & van Gelder, 2015; Hafermalz, 2021; Kayas et al., 2008), previous frameworks overlook or underplay their influence on shaping the characteristics of surveillance (i.e., Ball, 2002; Ball & Margulis, 2011; Ravid et al., 2020; Sewell, 1998; Sewell et al., 2011; Sewell & Barker, 2006; Stanton, 2000). The following discussion therefore develops organisational culture, leadership, management, and employees as the key social elements shaping the characteristics of surveillance. Fig. 2 illustrates the elements of the social dimension, their relationship with the technological dimension, and how they shape the sociotechnical characteristics of workplace surveillance.

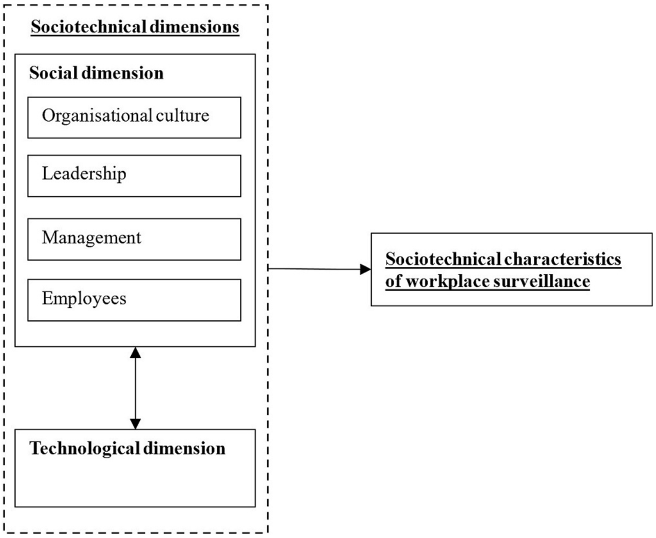


**Fig. 2.** The social dimension of workplace surveillance.

#### *4.1.1. Organisational culture*

Organisational culture includes the shared assumptions, beliefs, norms, and values that influence how organisations behave and function (Schein, 2009). Organisational interventions that are congruent with these shared assumptions, beliefs, norms, and values can produce positive responses from employees, managers, and leaders; however, if organisational interventions are incongruent with these shared cultural elements, then they can create negative responses (Ravid et al., 2020). Indeed, through their everyday social interactions, employees make sense of surveillance by assigning meaning to their experiences and embedding them in the history of the organisation's culture (Ellis & Taylor, 2006). Ball and Margulis (2011) develop the concept of *negotiated order* to explain how these everyday social interactions shape the appropriation of surveillance by groups of employees who then embed it within an organisation's culture. Empirical research has also shown how organisational culture shapes the characteristics of workplace surveillance. Kayas et al. (2008), for example, describe how senior management decided not to use an enterprise system to monitor employees' performance, despite providing the digital infrastructure, because the organisation's culture did not emphasise strict performance targets or monitoring. Hafermalz (2021) suggests that organisational culture can engender a fear of being left out, overlooked, ignored, or banished, which acts as a regulatory force that shifts the responsibility for visibility, in terms of competitive exposure and existential recognition, onto employees. Elsewhere, Alder (2001) argues that a culture open to involving employees in the design and configuration of surveillance systems can improve attitudes towards monitoring.

#### *4.1.2. Leadership*

Leadership is a social process that involves an individual influencing a group of people to achieve a common goal; in this sense, leadership is not a unidirectional phenomenon, but an interactive activity in which a leader affects others and is simultaneously affected by them through a reciprocal process (Northouse, 2022). Although empirical research has shown the significant impact different leadership approaches and styles have on shaping the characteristics of workplace surveillance, it is not accounted for in previous frameworks. For example, in their study of the triggers influencing leadership's decision to monitor subordinates, Alge et al. (2004) reveal that leaders are more likely to intensely monitor when dependence on subordinates is high or future performance expectations are low. They also found that leaders are more likely to deploy *secretive monitoring* practices when dependence on subordinates is high or the propensity to trust is low. In a different vein, Liao and Chun (2016) indicate that surveillance practices that stimulate perceptions of trust can foster a supporting environment for subordinate innovation. This occurs should leadership adopt *interactional monitoring* practices that facilitate 'the gathering of subordinate work progress or outcome information that involves the solicitation of information directly from subordinates' (Liao & Chun, 2016, p. 171). The leadership intervention model developed by Zohar (2002) also shows how leaders introduce surveillance practices to monitor and reward subordinate safety performance by prioritising safety over competing goals such as speed or schedules.

#### *4.1.3. Management*

Management is a human activity involving managers coordinating, directing, overseeing, supporting, and supervising the efforts of others to ensure organisational expectations are achieved (Merchant, 1982; Robbins et al., 2014). Although it is unaccounted for in previous surveillance frameworks, empirical research recognises the significant impact management has on shaping the characteristics of surveillance.

Managers play a vital role in creating monitoring practices to enforce contractual arrangements and minimise embezzlement and fraud (Merrett & Seltzer, 2000) or subjecting religious employees to a matrix of managerial, peer, and religious community gazes (Wasserman & Frenkel, 2020). Interestingly, Pierre et al. (2008) argue that if managers are risk averse, then there is a greater chance they will deploy intensified monitoring practices, while Dominguez-Martinez et al. (2014) suggest the monitoring practices engendered by managers are shaped by their interest alignment with employees. Webb and Palmer (1998) even argue that managers could consent to changing the characteristics of surveillance if it does not conflict with their interests.

### 4.1.4. Employees

Although previous frameworks do not fully account for the impact employees have on shaping surveillance characteristics, their role is widely reported in empirical studies. In fact, Ball (2010) argues that involving employees in the design of surveillance practices and policies will ensure they have a better chance of being accepted. Involving employees in the design of surveillance practices can even improve performance (Parker & Grote, 2022) and eliminate perceptions that it violates trust relations between employees and employers (Westin, 1992). Do et al. (2024) even argue for employee involvement in the design of surveillance tools, so they can be used to monitor people in power and fight back against the harms and consequences of surveillance. In a different vein, empirical studies show how employees can shape the characteristics of surveillance through acts of resistance. Indeed, resistance activities can change surveillance characteristics if employees are able to turn the table so they can surveil their own managers and employers (Clawson & Clawson, 2017; Taylor & Dobbins, 2021). Neto et al. (2018) even found that, depending on the request made, managers can alter the characteristics of surveillance to avoid disruption caused by resistance activities. However, employees who resist surveillance because they feel unnoticed as individuals could inadvertently provide management with a justification for increased surveillance (Anteby & Chan, 2018).

## 4.2. The technological dimension

Although digital technology shapes the characteristics of surveillance (Ball, 2021; Kayas, 2023; Manokha, 2020), previous frameworks do not fully consider the influence the different elements of technology have on shaping its characteristics, often positioning it as a background concern (if positioning it at all) (i.e., Ball & Margulis, 2011; Ravid et al., 2020; Sewell, 1998; Sewell et al., 2011; Sewell & Barker, 2006; Stanton, 2000). This study develops focus, boundary, datafication, automation, timeline, and frequency as the key elements of digital technology shaping the characteristics of surveillance. Crucially, while each of these elements provides the digital infrastructure needed to deploy surveillance, social actors within an organisation's particular social context influence which technology is implemented to surveil, how it is configured to surveil, and, thus, the characteristics of surveillance. Fig. 3 illustrates the technology elements, their interaction with the social dimension, and how they shape the sociotechnical characteristics of workplace surveillance.

### 4.2.1. Focus

Focus refers to the ability of digital technology to monitor the activities of individuals (i.e., employees, managers, and leaders) and/or collectives (e.g., teams, executive committees, board directors, departments, divisions, and working groups). For example, information systems that can focus on the performance of both individuals and teams working in call centres (Bain & Taylor, 2000; Ellway, 2013) or enterprise systems that can focus on the performance of individuals, teams, departments, and divisions (Kayas et al., 2008; Kayas et al., 2019). More recently, machine learning algorithms have provided organisations with the ability to focus on individuals with laser precision, by capturing customer data, locational data, and performance data, and connecting them with algorithmic decision making (Newlands, 2021). Firms can now also collect biometric data through wearable devices, allowing them to focus on the health and wellness of individual leaders, managers, and employees (e.g., pulse, sleep, and respiration) (Mettler, 2023).

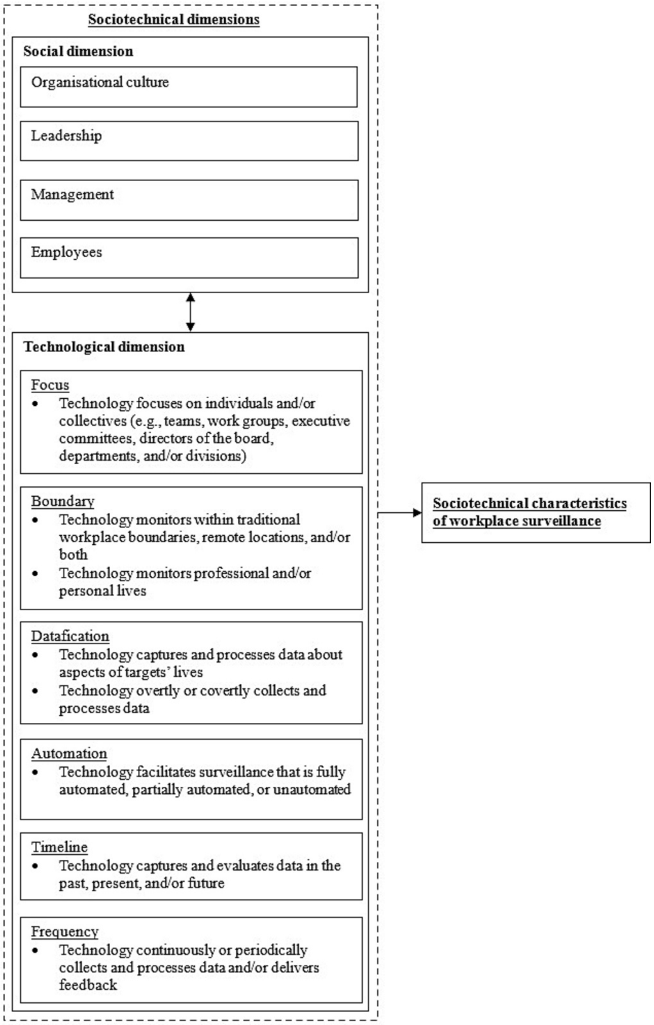

Sociotechnical dimensions
Social dimension
Organisational culture
Leadership
Management
Employees
Technological dimension
Focus
• Technology focuses on individuals and/or collectives (e.g., teams, work groups, executive committees, directors of the board, departments, and/or divisions)
Boundary
• Technology monitors within traditional workplace boundaries, remote locations, and/or both
• Technology monitors professional and/or personal lives
Datafication
• Technology captures and processes data about aspects of targets' lives
• Technology overtly or covertly collects and processes data
Automation
• Technology facilitates surveillance that is fully automated, partially automated, or unautomated
Timeline
• Technology captures and evaluates data in the past, present, and/or future
Frequency
• Technology continuously or periodically collects and processes data and/or delivers feedback
Sociotechnical characteristics of workplace surveillance

**Fig. 3.** The technological dimension of workplace surveillance.

### 4.2.2. Boundary

Boundary is a multifaceted concept. It refers to the ability of digital technology to monitor leaders, managers, and employees within the traditional boundaries of the workplace. For example, using technology to monitor the ethical use of sales systems within the workplace (Bush et al., 2010) or tracking the location of doctors and nurses within hospitals (Coles, 2016). Boundary also refers to the ability of technology to track those who work remotely. For instance, algorithmic fleet management systems that capture and transmit data on driver location and behaviour (Levy, 2015) or customer relationship management systems that monitor salespeople's performance when visiting clients offsite (Leclercq-Vandelannoitte, 2017). Crucially, boundary also refers to the ability of technology to peer into the personal and professional lives of leaders, managers, and employees. For example, algorithmic technology that blurs private and professional boundaries through communication systems designed to control employees (Newlands, 2021).

### 4.2.3. Datafication

Datafication is the process of capturing aspects of a person's life and transforming them into data to realise new forms of value (Mayer-Schoenberger & Cukier, 2013). In the context of workplace surveillance, datafication refers to the ability of technology to overtly or covertly capture data to monitor and scrutinise the behaviours, emotions, location, performance, health, and wellness (to name a few) of leaders, managers, and employees. Datafication processes then transform these data into actionable insights that inform organisational decisions. For example, firms data-mining CVs to evaluate job candidates (Searle, 2006) or armies collecting performance data to measure the effort of recruits (Fafchamps & Moradi, 2015).

#### 4.2.4. Automation

Automation refers to the ability of digital technology to remove humans from surveillance practices, by fully or partially automating data collection, interrogation, and evaluation. This includes intelligent technology transforming the nature of work through surveillance processes (Rydzik & Kissoon, 2021) or AI algorithms automating performance monitoring practices (Kayas, 2024). Indeed, the *algorithmic gaze* replaces human observations with automated processes that reduce or eliminate managerial oversight of workforces (Kellogg et al., 2020; Newlands, 2021; Rydzik & Kissoon, 2021; Todolí-Signes, 2019). Algorithmic technology can even automate decision-making activities related to recruitment, promotions, and dismissals (e.g., Cameron & Rahman, 2022; Todolí-Signes, 2019).

#### 4.2.5. Timeline

Timeline refers to the capacity of technology to provide information about leaders, managers, and employees in the past, present, and future. Analytics technology plays a vital role in facilitating the timeline element of workplace surveillance (Coolen et al., 2023). From a descriptive perspective, analytics is used to monitor the past and present performance of academics (e.g., Kayas et al., 2020), board directors (e.g., Kayas, 2023), customer service advisors (e.g., Bhave, 2014), public sector employees (e.g., Kayas et al., 2019), soldiers (e.g., Fafchamps & Moradi, 2015), and truck drivers (e.g., Levy, 2015), to name a few. Analytics and simulation technology also support the timeline dimension by providing organisations with the means to predict how leaders, managers, and employees will behave or perform in the future. For example, predicting which employees will have positive emotions during customer interactions (Bromuri et al., 2021), which job candidates are a good fit for an employer (Berkelaar & Buzzanell, 2014), and which employees will achieve performance targets (Burtscher et al., 2011; Seppänen et al., 2025).

#### 4.2.6. Frequency

Frequency refers to the level of regularity with which digital technology captures data about leaders, managers, and employees, as well as the regularity with which it delivers feedback (Office of Technology Assessment, 1987; Ravid et al., 2020; Stanton, 2000). Digital technology could, for example, periodically capture data through batch processing systems or legacy systems (Kayas et al., 2019). More recently, technological advances have transformed the body into a data source, allowing employers to continually capture data on employees' work and non-work-related activities (Mettler, 2023). Organisations, for instance, can continuously collect biometric data through electronic fingerprints, hand geometry, and facial recognition to monitor employees' attendance, identity, and location (Ball, 2010). Using wearable devices, organisations can also continuously collect health and wellness data that connect behaviours (e.g., physical activity) and the measurement of body functions (e.g., pulse and respiration) with algorithmic decision making (Mettler, 2023).

Technology can also provide surveillance targets with high or low levels of feedback about work tasks through notifications, messages, emails, or reports delivered periodically or continuously. In some industries, employees receive high levels of feedback through continuous smartphone notifications, informing them about new work tasks, task requirements, and employer and customer performance ratings (Chan, 2019; Newlands, 2021). Elsewhere, digital technology is used to produce scorecards that continuously transmit and display feedback to employees, including hours of service and other performance indicators (Levy, 2015). At the other end of the spectrum, technology can deliver low levels of periodic feedback. For example, enterprise systems configured to deliver monthly or annual performance reports to employees (Kayas et al., 2019) or teaching evaluation systems designed to provide academics with feedback at the end of a semester (Kayas et al., 2020).

### 4.3. The sociotechnical characteristics of workplace surveillance

This section develops the different characteristics of workplace surveillance (i.e., purpose, observer, target, direction, transparency, and intrusiveness) to reveal how each of the elements of the social and technological dimensions interact to shape each of these characteristics within particular organisations (Fig. 4). An updated and extended version of the Office of Technology Assessment (1987) model of workplace surveillance is also developed, showing how recent surveillance practices monitor, measure, and evaluate the performance, behaviour, and personal characteristics of employees, managers, and leaders (Fig. 5). The sociotechnical dimensions (Fig. 4) and the extended Office of Technology Assessment (1987) model (Fig. 5) are then integrated to produce the sociotechnical framework of workplace surveillance (Fig. 6).

#### 4.3.1. Purpose

Purpose refers to the explicit or perceived motivation or rationale for workplace surveillance. More than any of the other characteristics, purpose most clearly illuminates how organisations value their leaders, managers, and employees, as well as what they expect from them (Ball, 2010; Ravid et al., 2020). The factors motivating the decision to use workplace surveillance are categorised using the Office of Technology Assessment's (1987) three key purposes: performance, behaviour, and personal characteristics.

The purpose of surveillance can have significant implications. For example, employees are more likely to trust their employer and accept surveillance if they are monitored to support decisions around rewards while exposing antisocial behaviours like favouritism (Kayas, 2023; Kayas et al., 2020). However, surveillance implemented to prevent employee loafing can communicate a lack of mistrust (Glassman et al., 2015), while surveillance used to manage performance can reduce employee autonomy and commitment (Cameron & Rahman, 2022). Perceptions surrounding the purpose of surveillance can also lead to workforce resistance. In the public sector, for example, government employees may resist surveillance implemented for the purpose of increasing efficiency if it damages the quality of the services delivered to citizens (Kayas et al., 2019).

From a sociotechnical perspective, the purpose of surveillance is not shaped by technology. It is shaped by the actors within an organisation's particular social context. Especially leaders, who are responsible for ensuring that an organisation fulfils its expectations and obligations (Northouse, 2022). Should an organisation require constant product innovation to grow, for example, then leaders may decide to implement and configure surveillance technologies that encourage creativity and innovation (Liao & Chun, 2016). In a different setting, leaders could, for instance, introduce surveillance technologies to reduce shirking if perceptions of effort are low (Xiang, 2020). The purpose of surveillance can also be shaped by external actors. Kayas et al. (2019), for example, show how policy decisions by the central government required leaders in local authorities to implement enterprise systems to monitor public sector employees.

Alongside leadership, management can shape the purpose of surveillance because they too are responsible for ensuring organisational expectations are achieved (Merchant, 1982; Robbins et al., 2014). Kayas

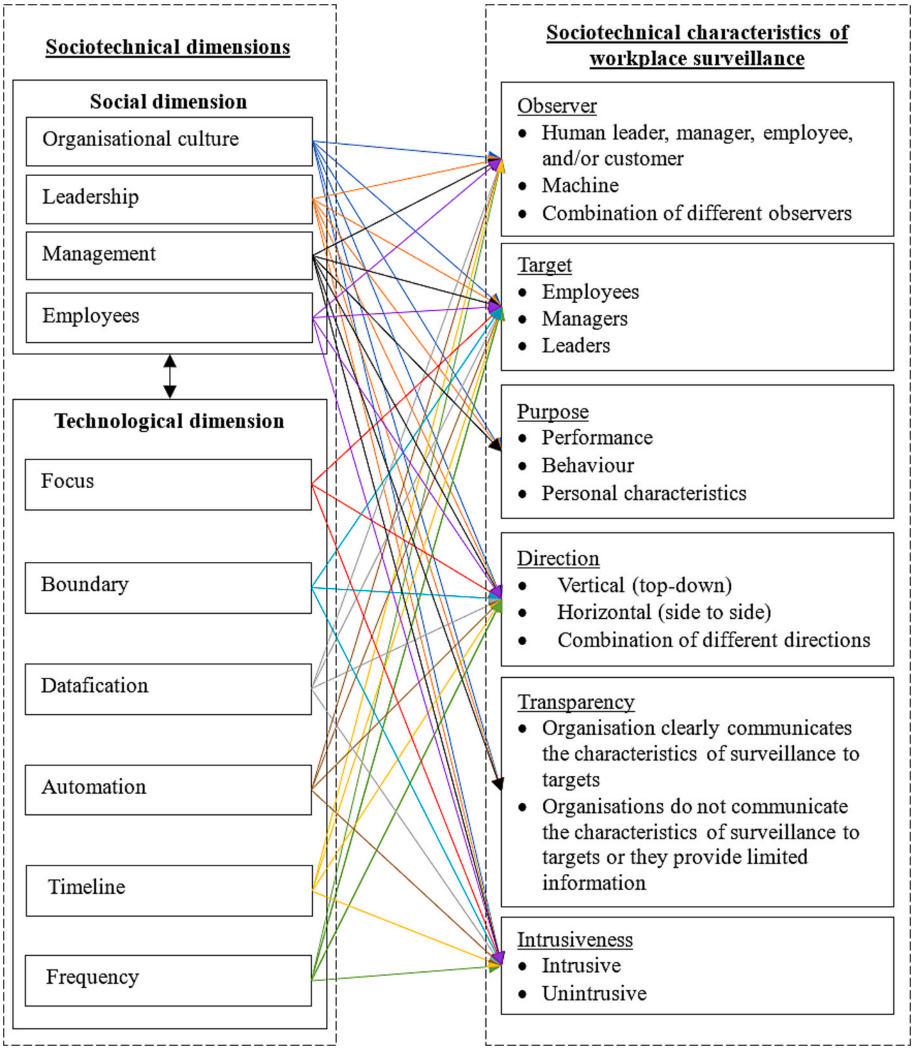

Sociotechnical dimensions
Social dimension
Organisational culture
Leadership
Management
Employees
Technological dimension
Focus
Boundary
Datafication
Automation
Timeline
Frequency
Sociotechnical characteristics of workplace surveillance
Observer
• Human leader, manager, employee, and/or customer
• Machine
• Combination of different observers
Target
• Employees
• Managers
• Leaders
Purpose
• Performance
• Behaviour
• Personal characteristics
Direction
• Vertical (top-down)
• Horizontal (side to side)
• Combination of different directions
Transparency
• Organisation clearly communicates the characteristics of surveillance to targets
• Organisations do not communicate the characteristics of surveillance to targets or they provide limited information
Intrusiveness
• Intrusive
• Unintrusive

**Fig. 4.** The social and technological elements shaping the different characteristics of workplace surveillance.

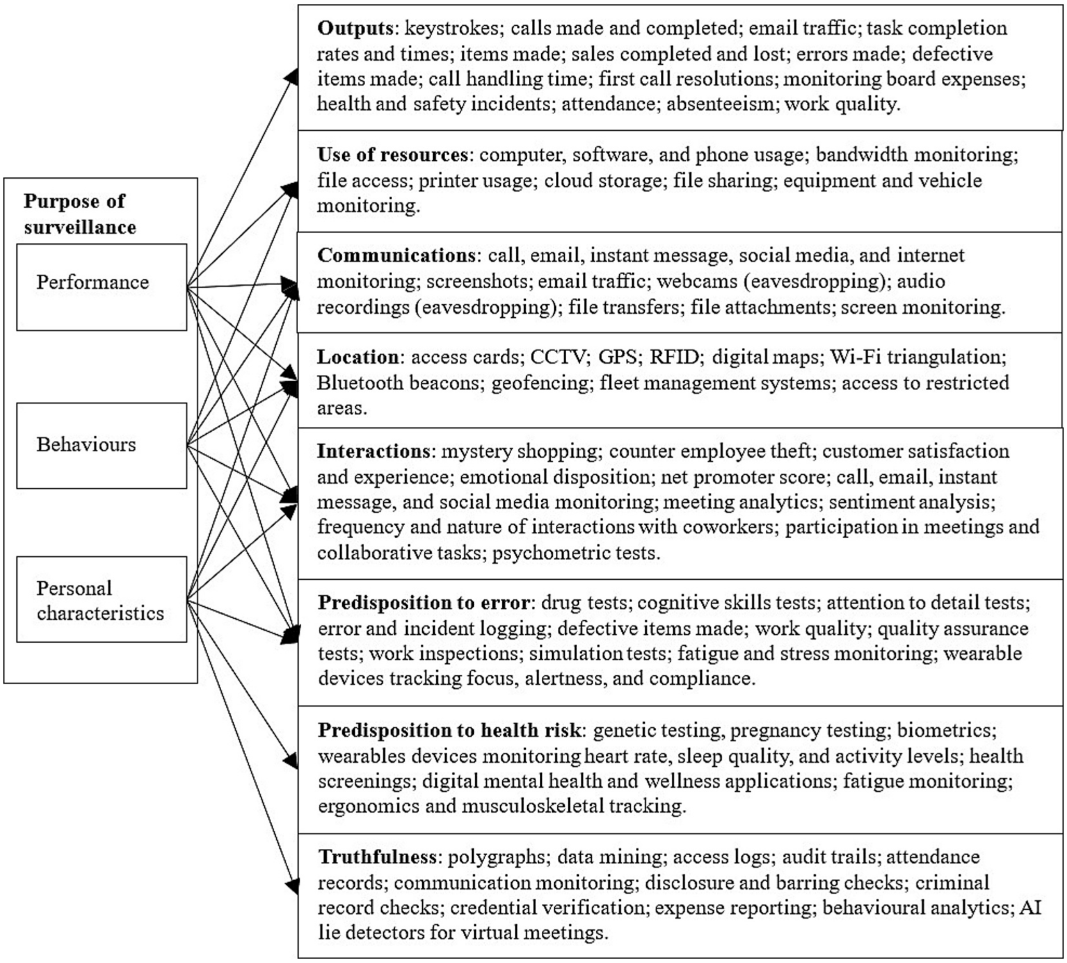
(2023), for example, identifies a range of factors shaping management's rationale for using electronic surveillance, including increasing performance, improving behaviours, reducing corruption, ensuring compliance, enhancing security, and improving customer satisfaction. Organisational culture also shapes the purpose of sociotechnical surveillance. While a culture emphasising safety, for example, can influence how surveillance technologies are configured to ensure the safety of employees (Collinson, 1999), a culture emphasising service quality over strict performance targets could lead to an organisation configuring technology such that it does not monitor the performance of employees or supervisors (Kayas et al., 2008).

### 4.3.2. *Observer*

Observer refers to the person(s) and/or technology that is watching over leaders, managers, and employees. Empirical research is dominated by studies focusing on managers as observers (e.g., Alder, 2001; Bain & Taylor, 2000; Levy, 2015). However, surveillance could also involve customers observing employees (e.g., Chan, 2019), leaders observing subordinates (e.g., Xiang, 2020), employees observing their peers (e.g., Ellway, 2013), or AI algorithmic systems automatically observing employees (e.g., Newlands, 2021). Importantly, observers can watch surveillance targets overtly or covertly. If the observer is watching overtly, then it is made clear to surveillance targets that they are being watched; however, if the observer is watching covertly, then surveillance targets are not informed (D'Urso, 2006).

The observer characteristic raises ethical concerns about autonomy, privacy, consent, and security because employees often lack awareness of the data used to observe them (Cameron & Rahman, 2022; Newlands, 2021). This reduces job satisfaction and encourages employees to resist through data obfuscation tactics designed to alter who can observe them and how they are observed (Chalykoff & Kochan, 1989; Kayas, 2023, 2024; Kellogg et al., 2020; Newlands, 2021). To mitigate against such resistance activities, employers should involve employees in discussions around the design of surveillance practices, provide ethical training, screen out job applicants who are opposed to monitoring, and communicate the characteristics of surveillance to targets of surveillance (Ball, 2010; Chalykoff & Kochan, 1989; West & Bowman, 2014). Engendering a participatory approach to the design of surveillance can even increase acceptance, improve performance, and reduce the likelihood that it will erode trust between employees and employers (Alder, 2001; Parker & Grote, 2022; Westin, 1992).

The interaction between both the social and technological dimensions shapes the observer characteristic of surveillance. From a social perspective, leaders have the power to decide, for example, whether managers should use technology to closely observe if employees adhere to an organisation's ethical principles (Sun et al., 2024) or achieve performance targets (Kayas et al., 2019). In higher education, university leaders have even recruited students as *mystery shoppers* to observe academics and provide management with performance information (Kayas et al., 2020). Managers can also shape the observer characteristic by



**Outputs**: keystrokes; calls made and completed; email traffic; task completion rates and times; items made; sales completed and lost; errors made; defective items made; call handling time; first call resolutions; monitoring board expenses; health and safety incidents; attendance; absenteeism; work quality.

**Use of resources**: computer, software, and phone usage; bandwidth monitoring; file access; printer usage; cloud storage; file sharing; equipment and vehicle monitoring.

**Communications**: call, email, instant message, social media, and internet monitoring; screenshots; email traffic; webcams (eavesdropping); audio recordings (eavesdropping); file transfers; file attachments; screen monitoring.

**Location**: access cards; CCTV; GPS; RFID; digital maps; Wi-Fi triangulation; Bluetooth beacons; geofencing; fleet management systems; access to restricted areas.

**Interactions**: mystery shopping; counter employee theft; customer satisfaction and experience; emotional disposition; net promoter score; call, email, instant message, and social media monitoring; meeting analytics; sentiment analysis; frequency and nature of interactions with coworkers; participation in meetings and collaborative tasks; psychometric tests.

**Predisposition to error**: drug tests; cognitive skills tests; attention to detail tests; error and incident logging; defective items made; work quality; quality assurance tests; work inspections; simulation tests; fatigue and stress monitoring; wearable devices tracking focus, alertness, and compliance.

**Predisposition to health risk**: genetic testing, pregnancy testing; biometrics; wearables devices monitoring heart rate, sleep quality, and activity levels; health screenings; digital mental health and wellness applications; fatigue monitoring; ergonomics and musculoskeletal tracking.

**Truthfulness**: polygraphs; data mining; access logs; audit trails; attendance records; communication monitoring; disclosure and barring checks; criminal record checks; credential verification; expense reporting; behavioural analytics; AI lie detectors for virtual meetings.

**Fig. 5.** Sociotechnical surveillance practices used to monitor, measure, and test employees, managers, and leaders.
Adapted from the Office of Technology Assessment (1987) and Ball (2010).

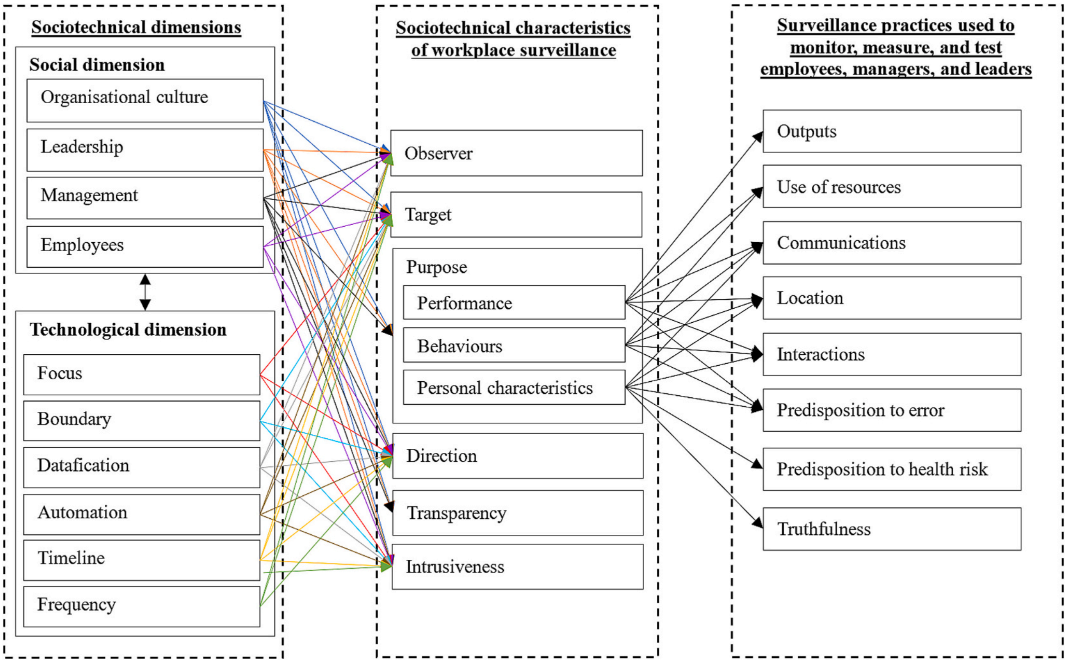


**Fig. 6.** The sociotechnical framework of workplace surveillance.

deciding, for instance, whether employees are subjected to their gaze or the gaze of their peers (Wasserman & Frenkel, 2020). Furthermore, should employees be involved in the design of surveillance practices, they too could influence who can observe (Do et al., 2024; Parker & Grote, 2022). Crucially, the observer characteristic can be shaped by those employees who resist surveillance. Newlands (2021), for example, shows how delivery workers resist algorithmic surveillance by engaging in individual and collective activities that obscure algorithmic observations, including swapping devices and temporarily switching devices off. Newlands also explains how delivery workers can resist observations by understanding the datafication parameters of algorithmic surveillance (i.e., what data is captured and how it is processed) to generate spaces that make them invisible on digital maps used to track their location.

Organisational culture also shapes the observer characteristic. In the police, for example, a culture of 'turning a blind eye' to certain behavioural deviations has resulted in senior police leaders establishing internal affairs divisions, where senior officers are given the power to observe and scrutinise subordinate behaviour (Cabral & Lazzarini, 2015). Organisations with highly centralised cultural contexts, manifesting in tall management structures and instrumental control systems, are more likely to observe employees; however, organisations with more decentralised cultural contexts, resulting in flatter hierarchies and information systems that empower employees to take collective responsibility, are more likely to engender peer observations (Barron & Gjerde, 1997; Sewell, 1998). Elsewhere, it has been shown that if an organisation's culture encourages peers to scrutinise team production with information systems, then it can engender peer observations (Barron & Gjerde, 1997).

Depending on the technology available in an organisation and its configuration by actors within their particular social context, digital technology can also influence the observer characteristic of surveillance. Indeed, the datafication capabilities of digital technology determine what data are collected, whether they are transformed into scrutable information, and whether subsequent observations are overt or covert (Mayer-Schoenberger & Cukier, 2013; Singh, 2024). Manufacturing firms, for example, could implement digital visualisation boards, so managers can collect data to observe shopfloor workers, transform them into useful information highlighting any problems, and support decision-making (Clausen, 2023). From an automation perspective, actors could decide to implement digital technology that provides the means to engender a fully automated or partially automated machine observer (Kayas, 2024). Algorithmic technology using AI algorithms, for example, could be used to replace humans by fully automating the role of the observer through the collection and analysis of the data needed to surveil leaders, managers, and employees (Newlands, 2021). In terms of the timeline element, social actors decide which technology to implement, how it is configured, and, thus, when observers can watch i.e., in the past, present, and/or future (Manokha, 2020). The inherent capabilities of digital technology and its subsequent configuration by actors also influence the frequency with which data are provided to observers (Bhave, 2014).

### 4.3.3. *Target*

Target refers to the person or persons subjected to surveillance (e.g., employees, managers, and leaders), what surveillance practices target about them (e.g., productivity), and why they are targeted (e.g., to improve performance). Empirical studies show how targeting employees with surveillance can increase anxiety and stress (Schleifer & Shell, 1992; Smith et al., 1992), reduce employee job satisfaction and morale (Chalykoff & Kochan, 1989; da Cunha et al., 2015), and erode trust between employees and employers (Sewell, 1998). Furthermore, if surveillance practices target data on employee internal private states, such as their beliefs, likes, emotions, and well-being, then they are more likely to resist (Mettler, 2023).

Crucially, biases related to people's characteristics and identities (e.g., age, ethnicity, gender, nationality, race, and sex) are embedded in algorithmic surveillance systems (Cameron & Rahman, 2022; Kellogg et al., 2020). This can impact targets in terms of recruitment (Searle, 2006) and disciplinary punishments (Newlands, 2021). These biases also have significant implications for organisations, including the erosion of trust, industrial action, reputational damage, and legal consequences that include financial liabilities. However, if employers include targets in the design of surveillance, transparently communicate the characteristics of surveillance to targets, provide ethical training, and minimise the biases embedded in surveillance systems through considered development processes (Ball, 2010; Parker & Grote, 2022; Ravid et al., 2020; West & Bowman, 2014), then surveillance can improve targets' organisational citizenship behaviour (Merrett & Seltzer, 2000), reduce bribery (Xiang, 2020), eliminate delinquent behaviours (de Vries & van Gelder, 2015), improve health and safety (Zohar, 2002), lower absenteeism rates (De Paola et al., 2014), and improve attitudes towards surveillance (Alder, 2001).

The interaction between the social and technological dimensions shapes the target characteristic. From a social perspective, leaders and managers have the power to decide which technology to implement to surveil targets, how the technology is configured to surveil targets, who to target for surveillance, what to target, and why to target them. They could, for example, decide to implement algorithmic surveillance systems that automatically target and evaluate employees (Kellogg et al., 2020) or introduce enterprise systems that target the performance of managers and employees (Kayas et al., 2019). Organisational culture also influences who is targeted by surveillance. If an organisation's culture exhibits low managerial trust in employees, for example, it could intensify the need to target them with surveillance technologies (Sun et al., 2024). Furthermore, if organisational culture encourages peer scrutiny within and between teams, it could lead to employees targeting their colleagues with digitally mediated surveillance practices (Barron & Gjerde, 1997; Ellway, 2013).

Employees can also influence who is subjected to surveillance by using technology to target their colleagues and engage in peer surveillance to assess their performance (Sewell, 1998). Employees can also target superordinates by turning their gaze to leaders and managers as an act of resistance (Clawson & Clawson, 2017; Taylor & Dobbins, 2021). For example, using social networks to target leaders and managers, capturing material about them to post online, and voicing dissenting views (Taylor & Dobbins, 2021). Counter-institutional websites or 'gripe sites' also provide employees with the means to target leaders and managers with surveillance (Gossett & Kilker, 2006). To avoid being targeted in this way, leaders and managers may respond by modifying surveillance practices to appease employees in the hope that it will prevent any further dissent (Neto et al., 2018).

From a technological perspective, the focus capabilities of digital technology influence who is targeted by surveillance. If technology is only able to focus on collectives, then regardless of whether actors want to focus on individuals, surveillance can only target collectives; however, if technology can focus on individuals and organisational actors want to focus on individuals, then the surveillance can be used to target individuals. The boundary element influences where leaders, managers, and employees are targeted. For instance, production technology could be implemented and configured by leaders and managers to target employee performance within the workplace (Sewell & Wilkinson, 1992). In a different vein, leaders and managers could decide to implement and use social media monitoring tools to target employees' personal lives (McDonald & Thompson, 2016). In terms of the datafication element, an organisation's digital infrastructure influences what aspects of targets' lives are captured and transformed into actionable insights. For example, targeting employees' location to improve efficiency (Coles, 2016; Levy, 2015) or targeting and evaluating employee stress from emotion patterns (Bromuri et al., 2021).

From an automation perspective, social context influences the decision to implement digital technology that can automatically surveil targets. Algorithmic technology, for instance, can be configured by leaders and managers to automatically collect data about employees, sort performers and underperformers into categories, and then target underperformers with intensified surveillance to ensure organisational expectations are achieved (Kayas, 2024; Lyon, 2003). The timeline element of digital technology influences whether someone is targeted for surveillance in the past, present, and/or future (Bromuri et al., 2021; Burtscher et al., 2011; Coolen et al., 2023), while the frequency capabilities of technology influence the regularity with which surveillance practices gather data about targets as well as the frequency with which feedback is delivered to targets (Office of Technology Assessment, 1987; Stanton, 2000).

### 4.3.4. *Direction*

Sewell (1998, 2012) identified two dimensions of workplace surveillance based on the direction of its operation: top-down (i.e., vertical) and side-to-side (i.e., horizontal). Vertical surveillance refers to a process in which superordinates monitor subordinates, while horizontal surveillance involves peer scrutiny. Research shows how peer surveillance can undermine performance, trust, and effort (De Jong & Elfring, 2010; Ellway, 2013), while vertical surveillance can increase employees' feelings of mistrust towards management and heighten feelings of anxiety and stress associated with instrumental performance targets (Kayas et al., 2020).

Both the social and technological dimensions shape the direction of surveillance. As with the other characteristics of workplace surveillance, leaders and managers have the power to shape the direction of surveillance. They could decide, for example, to use board intelligence systems that provide executives with the ability to capture data about other executives (horizontal) (Chen, 2016), enterprise systems that allow leaders to monitor managerial performance (vertical) (Kayas et al., 2019), performance monitoring systems that provide managers with information about employees (vertical) (Bain & Taylor, 2000; Ball & Margulis, 2011), or information systems that enable employees to monitor whether peers comply with security procedures (horizontal) (Herath & Rao, 2009).

Employees can also shape the direction of surveillance through resistance activities. Kayas et al. (2020), for instance, show how academics resist performance monitoring systems by refusing to promote teaching satisfaction surveys to students. This lowers response rates and reduces the data leaders have to evaluate academic performance (vertical). Employees can also use an organisation's digital infrastructure to shape the direction of surveillance should they decide to scrutinise their peers (horizontal) (Ellway, 2013). Furthermore, empirical research has shown how control systems embedded within organisational culture evolve in response to managerial changes to produce self-managing teams that perform peer surveillance (Barker, 1993).

The technological dimension also shapes the direction of surveillance. In terms of the focus element, choices around the selection and configuration of digital technology influence whether observers can focus on individuals or collectives either vertically or horizontally. Sewell (1998), for instance, explains how production systems allow managers to focus on employees (vertical), while allowing employees to focus on their peers (horizontal). The boundary capabilities of digital technology also influence the direction of surveillance. If leaders decide to use RFID tags coupled with digital maps, for example, it would allow them to monitor employees' location within workplace boundaries (vertical) (Coles, 2016), while the introduction of algorithmic technology would enable managers to monitor the performance of employees working remotely (vertical) (Cameron & Rahman, 2022; Levy, 2015). From a datafication perspective, the actors within an organisation's particular cultural context could influence the configuration of digital technology, so that it processes data on a subordinate's life and transforms them into actionable management insights (vertical) (Sewell, 2012).

Depending on the social context of an organisation, the automation capabilities of technology could shape the direction of surveillance. For example, leadership could decide to introduce technology to replace human managers with algorithms that automatically collect employee data and connect them to algorithmic decision making (vertical) (Newlands, 2021). In terms of the timeline element, actors within their particular social context decide whether surveillance technology is used to point vertically or horizontally in the past, present, and/or future. For example, leaders implementing workplace analytics to describe past and present productivity or predict future behaviours (Coolen et al., 2023; Manokha, 2020). From a frequency perspective, actors influence whether technology is used to provide observers with the means to continuously or periodically collect performance data that facilitate vertical or horizontal surveillance (Bhave, 2014).

### 4.3.5. *Transparency*

Transparency refers to the extent to which organisations inform surveillance targets about the characteristics of workplace surveillance (Ravid et al., 2020). Specifically, whether an organisation provides clear information about the purpose of surveillance, who is targeted, why they are targeted, who will observe them, how data are collected, whether data will be collected overtly or covertly, when data are collected, how data will be analysed, and what measures will be deployed in response should targets achieve or fail organisational expectations.

Transparency has a significant impact on the acceptance of surveillance by leaders, managers, and employees (Zweig & Webster, 2002), views on organisational fairness and justice (Alder et al., 2006), and perceptions of an organisation's internal reputation (Men, 2014). A lack of transparency can also erode trust between employees and employers (Sewell, 1998; Zainab et al., 2022), create a toxic work environment (Bennett & Raab, 2003), lower employee morale (da Cunha et al., 2015), and increase the likelihood of managers and employees engaging in resistance activities that undermine an organisation's capacity to function (Ball, 2010; Kafer, 2016; Kayas et al., 2019). To avoid these issues, employers should strive to be transparent with leaders, managers, and employees about the characteristics of surveillance and involve them in discussions about the design of surveillance practices (Ball, 2010; Parker & Grote, 2022; Ravid et al., 2020).

From a sociotechnical perspective, it is the social dimension alone that influences whether an organisation communicates the characteristics of surveillance to targets of surveillance. Although digital technology provides a mechanism for communicating with a workforce about transparency, decisions surrounding the level of transparency are an outcome of human activity. Indeed, leadership and management influence the extent to which an organisation is transparent about the characteristics of its surveillance practices (Bennis et al., 2008; Men, 2014; Zainab et al., 2022), for they decide whether to clearly articulate its characteristics or whether to provide little or no information. If leaders and managers decide to clearly communicate its characteristics to surveillance targets, then transparency is high; however, if leaders and managers only communicate limited information (or none at all), then transparency is low (Ravid et al., 2020). Moreover, should leaders engender a culture of candour (i.e., encouraging the free and timely flow of information to employees and managers), then it could increase the likelihood that the characteristics of surveillance are articulated to a workforce; however, should leaders create a culture that dissuades the free and timely flow of information, then it is less likely that the characteristics will be communicated (Bennis et al., 2008).

### 4.3.6. *Intrusiveness*

Intrusiveness refers to the psychological and physical invasion of autonomy or personal space through surveillance practices (Chandra et al., 2020; Charbonneau & Doberstein, 2020). Perceptions of the level of intrusiveness are affected by all the other characteristics of workplace surveillance. The degree of perceived intrusiveness varies, from passive surveillance practices (e.g., tracking computer login times) to more invasive forms (e.g., covert screen recording and social media monitoring). Intrusiveness is a significant characteristic of workplace surveillance, influencing whether leaders, managers, and employees perceive surveillance as fair or overreaching (Tham & Holland, 2022).

If employees perceive surveillance as intrusive, it can reduce employee autonomy, commitment, job satisfaction, morale, and trust (Chalykoff & Kochan, 1989; da Cunha et al., 2015; Schleifer & Shell, 1992; Sewell, 1998; Zainab et al., 2022). Ethical concerns are also raised by organisations requiring employees to consent to intrusive surveillance practices in exchange for employment (Gurley, 2022). Intrusive surveillance practices can even lead to unethical behaviours among managers worried about achieving performance targets (Bush et al., 2010). With employees expecting to be in control of the personal information they provide to employers (Bhave et al., 2019), privacy issues arise when employees are subjected to intrusive surveillance practices that capture increasingly personal and sensitive data that may not be related to work, such as employees' beliefs, likes, and emotions (Mettler, 2023). More than any of the other characteristics, intrusiveness is likely to foster acts of resistance. To avoid these issues and increase acceptance of surveillance, employers should transparently communicate the characteristics of surveillance to targets, involve them in discussions about the design of surveillance practices, provide ethical training, and ensure that performance appraisal processes are supportive and developmental, rather than instrumental and punitive (Ball, 2010; Chalykoff & Kochan, 1989; Parker & Grote, 2022; Ravid et al., 2020; West & Bowman, 2014).

Intrusiveness is shaped by the interaction between both the social and technological dimensions. From a social perspective, organisational culture influences whether intrusive surveillance practices are used. If trust in employees is low, for example, it could increase the likelihood that more invasive surveillance technologies are deployed (Sun et al., 2024). Elsewhere, it has been reported that if an organisation's culture does not support a developmental approach to performance appraisals, it is likely that the surveillance technologies deployed will be punitive and militaristic (Ball, 2010). In terms of leaders and managers, they too shape the intrusiveness characteristic when deciding, for example, whether to implement and use intrusive surveillance technologies such as emotional monitoring systems or AI lie detectors during virtual meetings. They also decide whether to be transparent with targets about the purpose of surveillance, what technology is used to surveil, how technology is configured to surveil, who is targeted for surveillance, why they are targeted, who will observe them, how surveillance data are collected, whether data will be collected overtly or covertly, when data are collected, how data will be analysed, who will analyse data, and what organisational measures could be deployed in response. Managers could also introduce intensified surveillance practices if they are risk averse (Pierre et al., 2008). Moreover, in some ultraorthodox settings, the intersectionality of gender and religion could encourage managers to expose women to intrusive surveillance practices that subjugate them with contradictory gazes (Wasserman & Frenkel, 2020). Employees can also engender intrusive surveillance practices if they observe the performance of their peers without consent (Kayas et al., 2020; Kayas et al., 2024).

The intrusiveness characteristic can even be shaped by resistance activities carried out by managers and employees. According to Ball (2010), for example, when call centre managers are subjected to intrusive surveillance, they sometimes resist by colluding with employees to avoid being targeted by surveillance. Elsewhere, Doolin (2004) shows how doctors resisted intrusive surveillance practices by challenging the validity of a medical information system designed to monitor clinical activity and manipulate behaviours. Doctors influenced the reinterpretation of the system through continual resistance, eventually relegating it to an insignificant role. However, in other organisational settings, such acts of resistance provide leaders and managers with a justification to further intensify surveillance (Anteby & Chan, 2018).

In terms of the technological dimension, the focus capabilities of digital technology shape the perceived level of intrusiveness (Charbonneau & Doberstein, 2020). If social actors decided to use technology to focus on collectives, then surveillance could be perceived as less intrusive; however, if they decided to use technology to focus on individuals with laser precision, surveillance could be perceived as intrusive (Ball, 2021; Ravid et al., 2020). In terms of boundary, if social actors decide to use technology that blurs the boundary between the personal and professional lives of leaders, managers, and employees, then it can affect the degree to which surveillance is perceived as intrusive (Zweig & Webster, 2002). Technology used to monitor the quality of work within an organisation (Bhave, 2014), for example, is less likely to be perceived as intrusive than monitoring personal social media use (McDonald & Thompson, 2016). From a datafication perspective, if digital technology captures and processes sensitive data (e.g., what an employee believes, likes, and how well, fit, and healthy they are), then surveillance is more likely to be perceived as intrusive because it is monitoring internal states that targets may consider private (Mettler, 2023). Covert datafication technologies (e.g., hidden cameras and keylogging without disclosure) are also more likely to foster perceptions that surveillance is intrusive because not knowing when or how targets are being observed can increase stress, erode trust, and reduce privacy (D'Urso, 2006; Singh, 2024).

Perceptions of intrusiveness are also shaped by the automation capabilities of digital technology. If leaders decided to implement algorithmic technology to automatically capture employee performance data, for example, it could be perceived as intrusive because it increases organisational control, resulting in surveillance targets resisting its effects (Cameron & Rahman, 2022; Kellogg et al., 2020). Elsewhere, executives have been shown to perceive sales technology as intrusive when it automatically monitors and scrutinises their compliance with ethical sales policies (Bush et al., 2010). In terms of timeline, digital technology that captures data about leaders, managers, and employees in the past and present may be perceived as less intrusive than technology that is configured by social actors to also make predictions and prescribe actions based on behaviours yet to have been committed. Finally, the frequency element of technology influences the degree to which surveillance is perceived as intrusive. If digital technology continually collects real-time data and/or delivers continual feedback, for example, it can make targets feel constantly watched; thus, increasing feelings of surveillance as intrusive (Ball, 2010; Charbonneau & Doberstein, 2020; Sewell et al., 2011).

## 5. Practical implications

The sociotechnical framework of workplace surveillance has a range of practical implications for organisations, leaders, managers, employees, and policy makers. From an organisational perspective, the framework offers practical recommendations for responsibly implementing sociotechnical surveillance practices that will reduce resistance, mitigate negative outcomes, improve trust between employers and employees, avoid ethical concerns, and increase the acceptance of surveillance. First, organisations should conduct an audit to assess current surveillance practices, their impact on leaders, managers, and employees, and how these practices align with organisational goals. Second, organisations should empower leaders, managers, and employees by fostering a participatory approach that encourages them to engage in discussions about the design and implementation of surveillance practices (Ball, 2010; Do et al., 2024; Parker & Grote, 2022). Third, organisations should consider employee perceptions around the perceived intrusiveness of surveillance practices and weigh their potential benefits against ethical concerns relating to autonomy, bias, privacy, consent, and unethical behaviours. Fourth, organisations should consider the vital role culture has in shaping surveillance characteristics to ensure surveillance practices align with employees' cultural beliefs, norms, values, and expectations. Fifth, organisations should develop transparent surveillance practices and policies that comply with legal and regulatory requirements (e.g., GDPR). Finally, organisations should conduct regular assessments to ensure they have adaptable surveillance practices and policies that change with organisational needs, technological advances, and legal and regulatory requirements.

The sociotechnical framework also highlights the need for clearer regulatory guidelines. Indeed, policymakers should move beyond traditional approaches to developing surveillance policies, which often regulate technologies (e.g., biometrics and AI) and data (e.g., GDPR), but overlook social factors shaping surveillance. Adopting a sociotechnical approach would allow policymakers to consider how organisational culture, leadership, management, and employees (not just data or technology) shape surveillance practices. Furthermore, policymakers should introduce *surveillance impact assessments* that go beyond current *data protection impact assessments*, which primarily focus on privacy and data protection, by explicitly considering the broader social implications of workplace surveillance.

## 6. Conclusions

This paper aimed to produce a new sociotechnical framework to explain how the social and technological dimensions within an organisation shape the characteristics of workplace surveillance. The sociotechnical framework indicates that both the social and technological elements shape the characteristics of workplace surveillance. Indeed, empirical research highlights the significant impact organisational culture, leadership, management, and employees have on shaping the characteristics of surveillance and, thus, were integrated into the framework. In doing so, this paper produces a conceptualisation of workplace surveillance that recognises the role of individuals and collectives at all levels along organisational hierarchies; thus, challenging traditional organisational structures by conceptualising surveillance as a sociotechnical phenomenon that shapes and is shaped by actors regardless of their hierarchical position. Empirical research also reports the major influence the elements of digital technology have on shaping the characteristics of surveillance and were therefore developed and integrated into the sociotechnical framework. Namely, focus, boundary, datafication, automation, timeline, and frequency. To recapitulate, the characteristics of surveillance include purpose, observer, target, direction, transparency, and intrusiveness. The main argument of this paper is that to understand the particular type of surveillance engendered in different organisational settings, it is essential to understand how the specific social and technological elements interact to shape each of the characteristics of surveillance.

### *6.1. Limitations and future research opportunities*

While this paper provides a valuable framework to analyse how the sociotechnical conditions shape the characteristics of workplace surveillance, as with any conceptual paper, it is constrained by its reliance on existing literature and the lack of empirical validation. Researchers are therefore encouraged to adopt the framework in qualitative and quantitative empirical studies to validate the framework's assumptions, relationships, and applicability in varied organisational settings. This could be done using case studies, surveys, interviews, or ethnographic studies. Longitudinal studies would also support the empirical validation of the framework, providing insight into how the social and technological dimensions shape and reshape surveillance characteristics over an extended period. Comparative studies would also provide an opportunity to empirically validate the framework in different sectors, industries, regions, and cultures to assess its generalisability and identify potential contextual variations.

Workplace surveillance engenders a multitude of outcomes and ethical concerns. It is beyond the scope of this paper to empirically examine how the sociotechnical characteristics of surveillance affect the various outcomes and ethical challenges for leaders, managers, and employees. To address this constraint, future research could draw on the framework to empirically examine how the sociotechnical dimensions in different organisations (1) shape the characteristics of surveillance and (2) their subsequent impact on particular outcomes and ethical challenges, such as autonomy, morale, privacy, consent, unethical behaviours, security, and trust. Such empirical studies could utilise qualitative or quantitative methods, including surveys, interviews, observations, experiments, and document analysis as well as mixed method studies.

Finally, this paper recognises that power permeates throughout the interactions between the social and technological dimensions of sociotechnical surveillance. Indeed, empirical studies have shown how and why employees actively resist the power exerted through surveillance practices (e.g., Cameron & Rahman, 2022; Kellogg et al., 2020; Levy, 2015). Consequently, this paper acknowledges that the unique power relationships between leaders, managers, and employees in different organisations can shape each characteristic of workplace surveillance. However, a detailed discussion is beyond the scope of this paper. To address this limitation, future empirical studies are encouraged to examine how power dynamics shape the interaction between the social and technological dimensions and the subsequent impact this has on shaping the characteristics of workplace surveillance.

## CRediT authorship contribution statement

**Oliver G. Kayas:** Writing – original draft, Project administration, Investigation, Formal analysis, Conceptualization. **Chin Eang Ong:** Writing – original draft. **H.M. Belal:** Writing – original draft.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgements

N/A.

## Data availability

No data was used for the research described in the article.

## References

Alder, G. S., Ambrose, M. L., & Noel, T. W. (2006). The effect of formal advance notice and justification on internet monitoring fairness: Much about nothing? *Journal of Leadership and Organizational Studies, 13*(1), 93–108. https://doi.org/10.1177/10717919070130011101

Alder, S. G. (2001). Employee reactions to electronic performance monitoring: A consequence of organizational culture. *The Journal of High Technology Management Research, 12*(2), 323–342. https://doi.org/10.1016/S1047-8310(01)00042-6

Alge, B. J., Ballinger, G. A., & Green, S. G. (2004). Remote control: Predictors of electronic monitoring intensity and secrecy. *Personnel Psychology, 57*(2), 377–410. https://doi.org/10.1111/j.1744-6570.2004.tb02495.x

Anteby, M., & Chan, C. K. (2018). A self-fulfilling cycle of coercive surveillance: Workers' invisibility practices and managerial justification. *Organization Science, 29*(2), 247–263. https://doi.org/10.1287/orsc.2017.1175

Bain, P., & Taylor, P. (2000). Entrapped by the "electronic panopticon"? Worker resistance in the call Centre. *New Technology, Work and Employment, 15*(1), 2–18.

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

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

Ball, K. (2016). Big data surveillance and the body-subject. *Body & Society, 22*(2), 58–81. https://doi.org/10.1177/1357034X15624973

Ball, K. (2021). *Electronic monitoring and surveillance in the workplace: Literature review and policy recommendations*. Publications Office of the European Union.

Ball, K., & Margulis, S. T. (2011). Electronic monitoring and surveillance in call centres: A framework for investigation. *New Technology, Work and Employment, 26*(2), 113–126.

Barker, J. R. (1993). Tightening the Iron cage: Concertive control in self managing teams. *Administrative Science Quarterly, 38*(3), 408–437.

Barron, J. M., & Gjerde, K. P. (1997). Peer pressure in an agency relationship. *Journal of Labor Economics, 15*(2), 234. https://doi.org/10.1086/209832

Bennett, C. J., & Raab, C. D. (2003). *The governance of privacy: Policy instruments in global perspective*. Routledge. https://doi.org/10.4324/9781315199269

Bennis, W., Goleman, D., O'Toole, J., & Biederman, P. W. (2008). *Transparency: How leaders create a culture of candor*. Jossey-Bass.

Bentham, J. (1791). *Panopticon or the inspection house*. T. Payne.

Berkelaar, B. L., & Buzzanell, P. M. (2014). Cybervetting, person–environment fit, and personnel selection: Employers' surveillance and sensemaking of job applicants' online information. *Journal of Applied Communication Research, 42*(4), 456–476. https://doi.org/10.1080/00909882.2014.954595

Bhave, D. P. (2014). The invisible eye? Electronic performance monitoring and employee job performance. *Personnel Psychology, 67*(3), 605–635. https://doi.org/10.1111/peps.12046

Bhave, D. P., Teo, L. H., & Dalal, R. S. (2019). Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management, 46*(1), 127–164. https://doi.org/10.1177/0149206319878254

Big Brother Watch. (2024). Bossware: The dangers of high-tech worker surveillance, and how to stop them. https://bigbrotherwatch.org.uk/wp-content/uploads/2024/09/BosswareWebVersion.pdf.

Bromuri, S., Henkel, A. P., Iren, D., & Urovi, V. (2021). Using AI to predict service agent stress from emotion patterns in service interactions. *Journal of Service Management, 32*(4), 581–611. https://doi.org/10.1108/JOSM-06-2019-0163

Burtscher, M. J., Kolbe, M., Wacker, J., & Manser, T. (2011). Interactions of team mental models and monitoring behaviors predict team performance in simulated anesthesia inductions. *Journal of Experimental Psychology. Applied, 17*(3), 257–269. https://doi.org/10.1037/a0025148

Bush, V., Bush, A. J., & Orr, L. (2010). Monitoring the ethical use of sales technology: An exploratory field investigation. *Journal of Business Ethics, 95*(2), 239–257. https://doi.org/10.1007/s10551-009-0357-9

Cabral, S., & Lazzarini, S. G. (2015). The "guarding the guardians" problem: An analysis of the organizational performance of an internal affairs division. *Journal of Public Administration Research and Theory, 25*(3), 797–829. https://doi.org/10.1093/jopart/muu001

Cameron, L. D., & Rahman, H. (2022). Expanding the locus of resistance: Understanding the co-constitution of control and resistance in the gig economy. *Organization Science, 33*(1), 38–58. https://doi.org/10.1287/orsc.2021.1557

Chalykoff, J., & Kochan, T. A. (1989). Computer-aided monitoring: Its influence on employee job satisfaction and turnover. *Personnel Psychology, 42*(4), 807–834. https://doi.org/10.1111/j.1744-6570.1989.tb00676.x

Chan, N. K. (2019). The rating game: The discipline of Uber's user-generated ratings. *Surveillance and Society, 17*(1–2), 183–190. https://doi.org/10.24908/ss.v17i1/2.12911

Chandra, S., Shirish, A., & Srivastava, S. C. (2020). Theorizing technological spatial intrusion for ICT enabled employee innovation: The mediating role of perceived usefulness. *Technological Forecasting and Social Change, 161*. https://doi.org/10.1016/j.techfore.2020.120320

Charbonneau, E., & Doberstein, C. (2020). An empirical assessment of the intrusiveness and reasonableness of emerging work surveillance Technologies in the Public Sector. *Public Administration Review, 80*(5), 780–791. https://doi.org/10.1111/puar.13278

Chen, Q. (2016). Director monitoring of expense misreporting in nonprofit organizations: The effects of expense disclosure transparency, donor evaluation focus and organization performance. *Contemporary Accounting Research, 33*(4), 1601–1624. https://doi.org/10.1111/1911-3846.12218

Clausen, P. (2023). Towards the industry 4.0 agenda: Practitioners' reasons why a digital transition of shop floor management visualization boards is warranted. *Digital Business, 3*(2), Article 100063. https://doi.org/10.1016/j.digbus.2023.100063

Clawson, D., & Clawson, M. A. (2017). IT is watching: Workplace surveillance and worker resistance. *New Labor Forum, 26*(2), 62–69. https://doi.org/10.1177/1095796017699811

Coles, L. C. O. (2016). Operational productivity and performance in English NHS acute hospitals: Unwarranted variations. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/499229/Operational_productivity_A.pdf.

Collinson, D. L. (1999). "Surviving the rigs": Safety and surveillance on North Sea oil installations. *Organization Studies, 20*(4), 579–600. https://doi.org/10.1177/0170840699204003

Coolen, P., van den Heuvel, S., Van De Voorde, K., & Paauwe, J. (2023). Understanding the adoption and institutionalization of workforce analytics: A systematic literature review and research agenda. *Human Resource Management Review, 33*(4), Article 100985. https://doi.org/10.1016/j.hrmr.2023.100985

da Cunha, J. V., Carugati, A., & Leclercq-Vandelannoitte, A. (2015). The dark side of computer-mediated control. *Information Systems Journal, 25*(4), 319–354. https://doi.org/10.1111/isj.12066

D'Urso, S. C. (2006). Who's Watching Us at Work? Toward a Structural–Perceptual Model of Electronic Monitoring and Surveillance in Organizations. *Communication Theory, 16*(3), 281–303.

De Jong, B. A., & Elfring, T. (2010). How does trust affect the performance of ongoing teams? The mediating role of reflexivity, monitoring, and effort. *Academy of Management Journal, 53*(3), 535–549. https://doi.org/10.5465/AMJ.2010.51468649

De Paola, M., Scoppa, V., & Pupo, V. (2014). Absenteeism in the Italian public sector: The effects of changes in sick leave policy. *Journal of Labor Economics, 32*(2), 337–360. https://doi.org/10.1086/674986

Do, K., Santos, M. D. L., Muller, M., & Savage, S. (2024). Designing gig worker sousveillance tools. In *Conference on human factors in computing systems, Honolulu, HI, USA*.

Dominguez-Martinez, S., Sloof, R., & von Siemens, F. A. (2014). Monitored by your friends, not your foes: Strategic ignorance and the delegation of real authority. *Games and Economic Behavior, 85*, 289–305. https://doi.org/10.1016/j.geb.2014.02.003

Doolin, B. (2004). Power and resistance in the implementation of a medical management information system. *Information Systems Journal, 14*(4), 343–362.

Ellis, V., & Taylor, P. (2006). You don't know what you've got till it's gone': Re-contextualising the origins, development and impact of the call Centre. *New Technology, Work and Employment, 21*(2), 107–122.

Ellway, B. P. W. (2013). Making it personal in a call Centre: Electronic peer surveillance. *New Technology, Work and Employment, 28*(1), 37–50. https://doi.org/10.1111/ntwe.12002

Fafchamps, M., & Moradi, A. (2015). Referral and job performance: Evidence from the Ghana colonial Army. *Economic Development and Cultural Change, 63*(4), 715–751. https://doi.org/10.1086/681276

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Penguin Books Ltd.

Gilson, L. L., & Goldberg, C. B. (2015). Editors' comment: So, what is a conceptual paper? *Group & Organization Management, 40*(2), 127–130. https://doi.org/10.1177/1059601115576425

Glassman, J., Prosch, M., & Shao, B. B. M. (2015). To monitor or not to monitor: Effectiveness of a Cyberloafing countermeasure. *Information & Management, 52*(2), 170–182. https://doi.org/10.1016/j.im.2014.08.001

Gossett, L. M., & Kilker, J. (2006). My job sucks: Examining Counterinstitutional web sites as locations for organizational member voice, dissent, and resistance. *Management Communication Quarterly, 20*(1), 63–90. https://doi.org/10.1177/0893318906291729

Granovetter, M. (1985). Economic action and social structure: The problem of embeddedness. *The American Journal of Sociology, 9*(3), 481–510.

Gurley, L. K. (2022). Amazon delivery drivers forced to sign 'biometric consent' form or lose job. *Vice Magazine*. Retrieved 25.02.2025 from https://www.vice.com/en/article/dy8n3j/amazon-delivery-drivers-forced-to-sign-biometric-consentform-or-lose-job.

Hafermalz, E. (2021). Out of the panopticon and into exile: Visibility and control in distributed new culture organizations. *Organization Studies, 42*(5), 697–717. https://doi.org/10.1177/0170840620909962

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Hirschheim, R. (2008). Some guidelines for the critical reviewing of conceptual papers. *Journal of the Association for Information Systems, 9*(8), 432–441. https://doi.org/10.17705/1jais.00167

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review*, 18–26. https://doi.org/10.1007/s13162-020-00161-0

Kafer, G. (2016). Reimagining resistance: Performing transparency and anonymity in surveillance. *Surveillance and Society, 14*(2), 227–239. https://doi.org/10.24908/ss.v14i2.6005

Kayas, O. G. (2023). Workplace surveillance: A systematic review, integrative framework, and research agenda. *Journal of Business Research, 168*, Article 114212. https://doi.org/10.1016/j.jbusres.2023.114212

Kayas, O. G. (2024). Algorithmic management: A surveillance perspective. In *Surveillance studies network conference, Ljubljana, Slovenia*, 28–31 May.

Kayas, O. G., Assimakopoulos, C., & Hines, T. (2020). Student evaluations of teaching: Emerging surveillance and resistance. *Studies in Higher Education, 47*(1), 1–12. https://doi.org/10.1080/03075079.2020.1725875

Kayas, O. G., Hines, T., McLean, R., & Wright, G. H. (2019). Resisting government rendered surveillance in a local authority. *Public Management Review, 21*(8), 1170–1190. https://doi.org/10.1080/14719037.2018.1544661

Kayas, O. G., Matikonis, K., Cranmer, E., & Campos, J. P. (2024). Socially negotiating privacy boundaries and academic identities. *Studies in Higher Education, 49*(7), 1241–1252. https://doi.org/10.1080/03075079.2023.2262507

Kayas, O. G., McLean, R., Hines, T., & Gillian, W. H. (2008). The panoptic gaze: Analysing the interaction between enterprise resource planning technology and organisational culture. *International Journal of Information Management, 28*(6), 446–452.

Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. *Academy of Management Annals, 14*(1), 366–410. https://doi.org/10.5465/annals.2018.0174

Leclercq-Vandelannoitte, A. (2017). An ethical perspective on emerging forms of ubiquitous IT-based control. *Journal of Business Ethics, 142*(1), 139–154.

Levy, K. E. C. (2015). The contexts of control: Information, power, and truck-driving work. *The Information Society, 31*(2), 160–174. https://doi.org/10.1080/01972243.2015.998105

Liao, E. Y., & Chun, H. (2016). Supervisor monitoring and subordinate innovation. *Journal of Organizational Behavior, 37*(2), 168–192. https://doi.org/10.1002/job.2035

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Open University Press.

Lyon, D. (2003). Surveillance as social sorting: Computer codes and mobile bodies. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination* (pp. 13–30). Routledge.

Manokha, I. (2020). The implications of digital employee monitoring and people analytics for power relations in the workplace. *Surveillance and Society, 18*(4), 540–554. https://doi.org/10.24908/ss.v18i4.13776

Mayer-Schoenberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. John Murray Publishers.

McDonald, P., & Thompson, P. (2016). Social media(Tion) and the reshaping of public/private boundaries in employment relations. *International Journal of Management Reviews, 18*(1), 69–84. https://doi.org/10.1111/ijmr.12061

Men, L. R. (2014). Internal reputation management: The impact of authentic leadership and transparent communication. *Corporate Reputation Review, 17*(4), 254–272. https://doi.org/10.1057/crr.2014.14

Merchant, K. A. (1982). The control function of management. *Sloan Management Review, 23*(4), 43–55.

Merrett, D. T., & Seltzer, A. (2000). Work in the financial services industry and worker monitoring: A study of the Union Bank of Australia in the 1920s. *Business History, 42* (3), 133–152. https://doi.org/10.1080/00076790000000270

Mettler, T. (2023). The connected workplace: Characteristics and social consequences of work surveillance in the age of datafication, sensorization, and artificial intelligence. *Journal of Information Technology, 39*(3), 547–567. https://doi.org/10.1177/02683962231202535

Neto, R. A.d. S., Ramos, A. S. M., & Dias, G. F. (2018). Resistance to electronic surveillance: The response of call center team managers. *Cadernos EBAPE.BR, 16*(4), 719–731. https://doi.org/10.1590/1679-395166874

Newlands, G. (2021). Algorithmic surveillance in the gig economy: The organization of work through Lefebvrian conceived space. *Organization Studies, 42*(5), 719–737. https://doi.org/10.1177/0170840620937900

Northouse, P. G. (2022). *Leadership: Theory and practice*. Sage Publications Ltd.

Office of Technology Assessment. (1987). The electronic supervisor: New technologies, new tensions. https://ota.fas.org/reports/8708.pdf.

Parker, S. K., & Grote, G. (2022). Automation, algorithms, and beyond: Why work design matters more than ever in a digital world. *Applied Psychology, 71*(4), 1171–1204. https://doi.org/10.1111/apps.12241

Parkes, H. (2023). Watching me, watching you: Worker surveillance in the UK after the pandemic. https://www.ippr.org/articles/worker-surveillance-after-the-pandemic.

Pierre, J. L., Rajan, M. V., & Ray, K. (2008). Optimal team size and monitoring in organizations. *Accounting Review, 83*(3), 789–822. https://doi.org/10.2308/accr.2008.83.3.789

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

Robbins, S. P., Bergman, R., Stagg, I., & Coulter, M. (2014). *Management*. Pearson.

Rydzik, A., & Kissoon, C. S. (2021). Decent work and tourism Workers in the age of intelligent automation and digital surveillance. *Journal of Sustainable Tourism*. https://doi.org/10.1080/09669582.2021.1928680

Schein, E. H. (2009). *The corporate culture survival guide*. John Wiley & Sons.

Schleifer, L. M., & Shell, R. L. (1992). A review and reappraisal of electronic performance monitoring, performance standards and stress allowances. *Applied Ergonomics, 23*(1), 49–53. https://doi.org/10.1016/0003-6870(92)90010-S

Searle, R. H. (2006). New technology: The potential impact of surveillance techniques in recruitment practices. *Personnel Review, 35*(3), 336–351. https://doi.org/10.1108/00483480610656720

Seppänen, S., Ukko, J., & Saunila, M. (2025). Understanding determinants of digital transformation and digitizing management functions in incumbent SMEs. *Digital Business, 5*(1), Article 100106. https://doi.org/10.1016/j.digbus.2025.100106

Sewell, G. (1998). The discipline of teams: The control of team-based industrial work through electronic and peer surveillance. *Administrative Science Quarterly, 43*(2), 397–428. https://doi.org/10.2307/2393857

Sewell, G. (2012). Organization, employees and surveillance. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies*. Routledge.

Sewell, G., & Barker, J. R. (2006). Coercion versus care: Using irony to make sense of organizational surveillance. *Academy of Management Review, 31*(4), 934–961.

Sewell, G., Barker, J. R., & Nyberg, D. (2011). Working under intensive surveillance: When does "measuring everything that moves" become intolerable? *Human Relations, 65*(2), 189–215. https://doi.org/10.1177/0018726711428958

Sewell, G., & Wilkinson, B. (1992). 'Someone to watch over me': Surveillance, discipline and the just-in-time labour process. *Sociology, 26*(2), 271–289.

Singh, S. (2024). Digital surveillance and valuation in datafied societies. In A. Krüger, T. Peetz, & H. Schaefer (Eds.), *The Routledge international handbook of valuation and society*. Routledge. https://doi.org/10.4324/9781003229353.

Smith, M. J., Carayon, P., Sanders, K. J., Lim, S. Y., & Legrande, D. (1992). Employee stress and health complaints in jobs with and without electronic performance monitoring. *Applied Ergonomics, 23*(1), 17–27. https://doi.org/10.1016/0003-6870(92)90006-H

Stanton, J. M. (2000). Reactions to employee performance monitoring: Framework, review, and research directions. *Human Performance, 13*(1), 85–113. https://doi.org/10.1207/S15327043HUP1301_4

Sun, U. Y., Park, H., & Yun, S. (2024). Ethically treated yet closely monitored: Ethical leadership, leaders' close monitoring, employees' uncertainty, and employees' organizational citizenship behavior. *Journal of Organizational Behavior, 45*(5), 702–719. https://doi.org/10.1002/job.2760

Taylor, C., & Dobbins, T. (2021). Social media: A (new) contested terrain between sousveillance and surveillance in the digital workplace. *New Technology, Work and Employment, 36*(3), 263–284. https://doi.org/10.1111/ntwe.12206

Tham, T. L., & Holland, P. (2022). Electronic monitoring and surveillance: The balance between insights and intrusion. In P. Holland, T. Bartram, T. Garavan, & K. Grant (Eds.), *The emerald handbook of work, workplaces and disruptive issues in HRM*. Emerald Publishing Limited. https://doi.org/10.1108/978-1-80071-779-420221051.

Todolí-Signes, A. (2019). Algorithms, artificial intelligence and automated decisions concerning workers and the risks of discrimination: The necessary collective governance of data protection. *Transfer: European Review of Labour and Research, 25* (4), 465–481. https://doi.org/10.1177/1024258919876416

de Vries, R. E., & van Gelder, J. L. (2015). Explaining workplace delinquency: The role of honesty-humility, ethical culture, and employee surveillance. *Personality and Individual Differences, 86*, 112–116. https://doi.org/10.1016/j.paid.2015.06.008

Wasserman, V., & Frenkel, M. (2020). The politics of (in)visibility displays: Ultra-orthodox women Manoeuvring within and between visibility regimes. *Human Relations, 73*(12), 1609–1631. https://doi.org/10.1177/0018726719879984

Webb, M., & Palmer, G. (1998). Evading surveillance and making time: An ethnographic view of the Japanese factory floor in Britain. *British Journal of Industrial Relations, 36* (4), 611–627. https://doi.org/10.1111/1467-8543.00110

West, J. P., & Bowman, J. S. (2014). Electronic surveillance at work: An ethical analysis. *Administration and Society*, 1–24. https://doi.org/10.1177/0095399714556502

Westin, A. F. (1992). Two key factors that belong in a macroergonomic analysis of electronic monitoring - employee perceptions of fairness and the climate of organizational trust or distrust. *Applied Ergonomics, 23*(1), 35–42. https://doi.org/10.1016/0003-6870(92)90008-J

Woodcock, J. (2021). *The fight against platform capitalism: An inquiry into the global struggles of the gig economy*. University of Westminster Press. https://doi.org/10.16997/book51

Xiang, W. (2020). Who will watch the watchers? On optimal monitoring networks. *Journal of Economic Theory, 187*. https://doi.org/10.1016/j.jet.2020.105018

Zainab, B., Akbar, W., & Siddiqui, F. (2022). Impact of transformational leadership and transparent communication on employee openness to change: Mediating role of employee organization trust and moderated role of change-related self-efficacy. *Leadership and Organization Development Journal, 43*(1), 1–13. https://doi.org/10.1108/LODJ-08-2020-0355

Zohar, D. (2002). Modifying supervisory practices to improve subunit safety: A leadership-based intervention model. *Journal of Applied Psychology, 87*(1), 156–163. https://doi.org/10.1037//0021-9010.87.1.156

Zuboff, S. (1988). *In the age of the smart machine: The future of work and power*. Basic Books Inc.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89.

Zweig, D., & Webster, J. (2002). Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. *Journal of Organizational Behavior, 23*(5), 605–633. https://doi.org/10.1002/job.157