

# The fragility of trust in digital workplace surveillance: Interpersonal and governance perspectives

## Abstract

Public sector organisations are increasingly using surveillance practices augmented with digital technologies, often justified through reform agendas centred around transparency, accountability, and performance improvement, yet the impact of surveillance on trust remains poorly understood. This paper examines how surveillance shapes trust within a local government authority through a qualitative case study drawing on interviews, observations, and documentation. The findings show that surveillance can reinforce trust when it supports fairness, protects employees, and improves decision making, but can erode trust when it is perceived as disproportionate, opaque, or selectively applied. The analysis also highlights how tensions between interpersonal experiences and governance narratives render trust a fragile and contested organisational condition. By moving beyond binary framings of trust versus control, this paper develops a multilevel account of how trust is shaped, negotiated, and destabilised in digitally surveilled public sector workplaces.

**Keywords:** workplace surveillance, employee trust, interpersonal trust, governance, transparency, accountability

## 1 Introduction

Public sector organisations are increasingly embedding surveillance practices augmented with digital technologies into the fabric of everyday work to monitor and evaluate employees' performance and behaviour (Rychwalska, Geoffrey, and Roszczynska-Kurasinska 2021; Lund-Tønnesen 2026; Flatøy and Lund-Tønnesen 2025). Technologies with monitoring capabilities, such as analytics, dashboards, enterprise systems, and performance management systems, have been implemented and justified through discourses of transparency, accountability, objectivity, and evidence based decision making, aligning with public sector reform agendas such as New Public Management and algorithmic governance, (Webster 2012; Hillo, Vento, and Erkkilä 2025; Pan, Song, and Jiang 2026). Within these reform agendas, surveillance functions as a governing mechanism that shapes how employees are perceived, judged, and managed (Miao et al. 2025).

In this sense, surveillance can be understood as a managerial response to the perceived absence or fragility of trust in employees, reflecting an attempt to compensate for distrust or to establish a basis upon which trust can be built (Zureike 2003; Alge and Hansen 2014; Introna 2003; Mettler 2024; Kayas, Chin, and Belal 2025). This in turn shapes how employees interpret managerial oversight, engage with institutional processes, and respond to surveillance practices that structure visibility and accountability (Bijlsma-Frankema, de Jong, and de Bunt 2008; Alder, Noel, and Ambrose 2006). It also shapes employee performance, engagement, participatory practices, burnout, gaming behaviours, cooperative willingness, fairness, commitment, trust, creativity, dignity, equality, and the ability to cope with risks from reform agendas, which all have significant implications for employees, managers, and organisations (Li 2015; Diefenbach 2009; Morales, Wittek, and Heyse 2015; Miao et al. 2025; Pan, Song, and Jiang 2026). Research also suggests that the effects of electronic monitoring are often mixed and contingent, rather than uniformly positive or negative, and are shaped by context, implementation, and interpretation (König 2025).

Previous surveillance research tends to position trust as a background concern, addressing it in relation to employee acceptance of surveillance or managerial perceptions of employee

reliability (Kayas 2023; Ball 2010). There is also a tendency to conceptualise surveillance and trust in oppositional terms, where the presence of surveillance is assumed to indicate a breakdown or absence of trust (Zureike 2003). This binary framing neglects the possibility that trust and surveillance may coexist in tension, producing interactions and contradictions that shape both interpersonal experiences and governance narratives. Indeed, research often isolates trust at a single level of analysis: a relational feature of manager–employee interactions (e.g., Schweitzer, Ho, and Zhang 2018; Bijlsma-Frankema, de Jong, and de Bunt 2008; Westin 1992; Alge and Hansen 2014; Flatøy and Lund-Tønnesen 2025; Perrier et al. 2024). Such studies overlook how trust operates across levels, simultaneously shaping interpersonal relationships and governance justifications. Public administration research on trust has similarly called for greater attention to the multilevel character of trust in public organisations, including the interplay between individual experiences and collective climates of trust (Perrier et al. 2024).

Recent public management research also suggests that the relationship between surveillance and trust is more complex than a simple erosion account implies. For example, quantitative studies show that employee perceptions of management’s trust can remain relatively robust to monitoring even when monitoring shapes turnover intention (Flatøy and Lund-Tønnesen 2025), and that public sector employees respond differently depending on whether monitoring is perceived as controlling or developmental (Miao et al. 2025). Quantitative research also indicates that more invasive forms of digital monitoring are not experienced uniformly, but vary across employees and organisational contexts (Abendroth, Schröder, and Meyer 2026). Elsewhere, Lund-Tønnesen (2026) argues that surveillance in public administration is increasingly embedded in wider governance arrangements rather than functioning only as a discrete managerial tool. While valuable, these studies fail to consider trust as a contested and fragile condition that is continually negotiated and easily destabilised by perceived breaches or contradictions between interpersonal and governance levels; particularly in public sector organisations which embed surveillance practices in their processes to satisfy political and public demands for transparency and accountability. This points to the need for qualitative research that can examine more closely how trust is interpreted, negotiated, and challenged within surveilled public sector settings, where current research still offers limited insight into the nuanced ways trust is negotiated across interpersonal and governance levels.

This paper’s aim is to examine how surveillance shapes trust in public sector organisations from both interpersonal and governance perspectives. Through a case study analysis focusing on employees and managers working in a UK local government authority, this paper addresses how trust is understood and enacted in relation to surveillance practices augmented with digital technology. Particular attention is paid to how trust features in the interpretation of surveillance, the interactions it mediates, and the organisational narratives used to justify it. In doing so, the paper develops a multilevel account of trust in surveillance settings as fragile and contested, arising from the tensions, interactions, and contradictions between interpersonal experiences and governance logics. This advances theorisations of trust by extending existing models beyond their conventional single level focus by integrating interpersonal and governance perspectives to explain how surveillance simultaneously builds, erodes, and mobilises trust.

This paper continues by providing an overview of the literature on workplace surveillance and trust. It then develops the study’s theoretical foundations by discussing trust from interpersonal and governance logic perspectives. Following this, the methodology is presented, and the findings are analysed. The study’s theoretical implications are then discussed, and a multilevel conceptualisation is offered that synthesises and extends existing theorisations of trust in

surveillance settings. The paper concludes by summarising its contributions, limitations, and future research opportunities.

## **2 Literature review**

### *2.1 Workplace surveillance and trust*

Workplace surveillance refers to the purposeful monitoring, recording, and evaluation of employee behaviour, performance, and personal characteristics (Ball 2010, 2003). It encompasses a range of control processes aimed at regulating conduct, enforcing accountability, and enhancing managerial oversight (Kayas, Chin, and Belal 2025). Long understood as a mechanism of control within the employment relationship, in the public sector, surveillance is also linked to the logics of accountability, transparency, and auditability (Hood 2007; Charbonneau and Doberstein 2020). Accordingly, it is often justified as a means of ensuring the efficient use of public resources, upholding service standards, and maintaining public confidence in decision making (Webster 2012). Yet, these rationales can obscure tensions surrounding fairness, proportionality, and professional autonomy, particularly when surveillance extends managerial oversight or amplifies performance pressures (Kayas et al. 2019; Bowman and West 2021). As a result, surveillance operates not only as a mechanism of control but also as a site where trust and accountability are continually negotiated.

Trust is a ubiquitous phenomenon surrounding workplace surveillance, functioning as both an antecedent and an outcome of the monitoring process (Alge and Hansen 2014). The expansion and normalisation of surveillance raises critical questions about how trust is constructed, maintained, and undermined in organisational settings (Kayas 2023; Ball 2010; Holland, Cooper, and Hecker 2015; König 2025). Surveillance is thus a proxy for the extent to which managers trust employees (Ball 2021; Westin 1992). Research indicates that surveillance is frequently introduced as a response to managerial concerns about employee performance and behaviour, especially when employees are not trusted to work independently or without supervision (Zureike 2003; Alder, Noel, and Ambrose 2006; Flatøy and Lund-Tønnesen 2025). Yet, the very introduction of surveillance not only affects employees' trust in their employer or manager, it also creates an atmosphere of mistrust (Ball 2010; Alder, Noel, and Ambrose 2006; Klöpffer and Rowe 2026). However, recent evidence suggests that this relationship is not uniformly damaging. Public sector research shows that employees may interpret similar monitoring practices differently depending on how they are enacted and experienced (Miao et al. 2025). Flatøy and Lund-Tønnesen (2025), for instance, found that employees' perceptions of management's trust in them remain relatively robust to monitoring, which they relate partly to the high-trust Norwegian context and to the possibility that some forms of monitoring are understood as appropriate or developmental rather than simply distrustful.

At the same time, employees often expect managers to observe their activities, set them objectives, and evaluate their performance (Ball 2010, 2022). Employees may even view surveillance as positively influencing trust if it enhances fairness, promotes accountability, guides reward decisions, and eliminates behaviours such as favouritism (Kayas 2023; Soomro et al. 2025). By providing an objective record that enables fair and transparent decision making, surveillance may foster greater trust in organisational processes and managerial accountability. However, surveillance lowers trust if it reaches into employees' personal lives, captures data about their characteristics beyond performance, compromises working practices, or negatively affects levels of control and autonomy (Kayas, Chin, and Belal 2025; Ball 2021; Glavin, Bierman, and Schieman 2024; Abendroth, Schröder, and Meyer 2026). This issue is further complicated by evidence that more invasive forms of digital monitoring, particularly those tied to performance evaluation and perceived constant surveillance, are not evenly distributed

across employees, but are shaped by organisational and job resources (Abendroth, Schröder, and Meyer 2026).

Surveillance therefore functions both as a response to mistrust and a mechanism that exacerbates it, reflecting managerial concerns about opportunistic employee behaviour while simultaneously signalling a lack of confidence in employee integrity (König 2025; Klöpfer and Rowe 2026). Low managerial trust in employees' expected performance leads to increased surveillance (Alder, Noel, and Ambrose 2006; Holland, Cooper, and Hecker 2015), yet this often produces a cycle in which increased surveillance further erodes employees' trust in management. According to Introna (2000), it is the political possibilities of surveillance itself, including the employee data selected to observe, the organisational values applied, the interests served, and the implicit nature of judgement processes, which makes employees default to a position of mistrusting management.

## 2.2 *Interpersonal trust*

At the interpersonal level, trust is a psychological state referring to the expectations and beliefs that individuals hold about the intentions, reliability, and integrity of others with whom they have direct relationships (McAllister 1995). In organisational settings, interpersonal trust develops through repeated interactions and plays a central role in shaping how employees interpret managerial behaviour, respond to oversight, and engage with organisational systems (Dirks and Ferrin 2001). Accordingly, Mayer, Davis, and Schoorman (1995) define trust as the willingness of one party to be vulnerable to the actions of another, based on the expectation that the latter will perform particular actions important to the trustor, irrespective of the ability to monitor or control them. Their model of trust identifies three core dimensions of perceived trustworthiness: (1) *ability*, i.e., the skills and competencies that enable responsible action; (2) *benevolence* i.e., the extent to which a trustee is believed to want to do good for the trustor; and (3) *integrity* i.e., the perception that the trustee adheres to a set of principles acceptable to the trustor. These dimensions shape how employees interpret managerial intent and judge the legitimacy of surveillance, highlighting how it is experienced through the filter of relational expectations, producing different interpretations depending on context.

Surveillance can influence how these three dimensions of trustworthiness are interpreted. For example, if employees believe that managers implement surveillance fairly, proportionately, and with a clear purpose, they may view it as a sign of managerial ability and competence, thereby reinforcing trust (Chory, Vela, and Avtgis 2016). Interpersonal trust in managers can also enhance organisational commitment and reduce turnover intention (Chen, Hsieh, and Chen 2014). If surveillance is used to support equitable performance assessment or to protect against misconduct, employees may interpret this as aligned with benevolent and principled managerial behaviour (Kayas 2023). In this sense, surveillance does not automatically signal mistrust but can operate as a mechanism through which trust is negotiated and even reinforced, depending on how it is framed and experienced (Miao et al. 2025). However, if surveillance is implemented without consultation or perceived as overreaching, it may convey managerial distrust, undermining employee autonomy, and lead to a decline in perceived benevolence or integrity (Kayas, Chin, and Belal 2025; Ball 2021). Public sector research similarly suggests that monitoring perceived as developmental can be more positively received than monitoring perceived as controlling, indicating that interpersonal trust judgements are shaped by how monitoring purpose is interpreted (Miao et al. 2025).

Interpersonal trust is also shaped by the broader organisational climate and employees' interpretive frameworks (Mayer, Davis, and Schoorman 1995; McAllister 1995). Employees

draw on prior interactions with managers, prevailing norms, and their sense of alignment with organisational values to assess whether surveillance is justified and fair (Kayas 2023; Dirks and Ferrin 2001; Kayas, Chin, and Belal 2025). Accordingly, in high trust environments, surveillance may be more readily accepted when it supports shared goals and accountability. In contrast, when interpersonal relationships are already marked by suspicion, surveillance is more likely to be interpreted as an expression of distrust (Miao et al. 2025; Flatøy and Lund-Tønnesen 2025). This underscores the tensions, with the same surveillance practices strengthening trust in one relational climate but undermining it in another. Public administration research also underlines that individual experiences of trust are shaped by wider collective climates, rather than emerging solely from isolated dyadic exchanges (Perrier et al. 2024).

### 2.3 *Trust as a governance logic*

Trust also operates as a governance logic used by employers to justify organisational processes, information systems, structures, and decision making practices (Gulati and Nickerson 2008). The notion of governance logic is rooted in institutional logics (Thornton, Ocasio, and Lounsbury 2012) and system trust (Giddens 1990), but is used here more narrowly to describe the normative and procedural rationalities through which trust becomes embedded in managerial discourse and surveillance systems, emphasising the internal narratives and rules that render these practices trustworthy. As a governance logic, trust becomes embedded in organisational narratives and managerial discourses, invoked to justify surveillance as fair, necessary, and aligned with organisational goals (Kritikos and Iphofen 2024). In this context, trust is less about the moral attributes of individual actors and more about cultivating confidence in the formal procedures, systems, practices, and technologies through which control is exercised (Giddens 2013). Surveillance practices are therefore not merely technical artefacts or operational tools, but political instruments that organisations frame as mechanisms of accountability, objectivity, and performance enhancement, with justifications often based on trust (Kayas, Chin, and Belal 2025). This draws attention to how governance logics of trust can collide with interpersonal interpretations, producing contradictions in how surveillance is understood. This dynamic aligns with research on digital surveillance governance, which argues that contemporary public sector reform increasingly embeds control, transparency, and personal data use within surveillance-based arrangements rather than treating surveillance as a discrete managerial technique (Lund-Tønnesen 2026).

In public sector organisations, the language of trust often intersects with dominant institutional logics of transparency, auditability, and risk management (Ferry and Midgley 2024; Natan-Krup and Mizrahi 2025; Bentzen, Winsvold, and Six 2026). Surveillance practices are thus rationalised as a means of securing public confidence, ensuring responsible use of taxpayer resources, and demonstrating procedural fairness (Kayas et al. 2019). They are also framed as trustworthy mechanisms that enable oversight without bias or favouritism (Gilliom and Monahan 2013). This rhetorical use of trust functions to pre-empt resistance by framing surveillance not as coercion, but as a form of organisational care and stewardship (Sewell and Barker 2006). Indeed, audit based systems are sustained not by their effectiveness alone, but by the cultural authority of trust they symbolically confer (Power 1997). Trust, in this framing, becomes both a discursive resource and an institutional shield, protecting surveillance from critique. In this respect, trust helps justify surveillance within wider public sector reform processes, even as those same processes intensify employee visibility and data-driven oversight (Lund-Tønnesen 2026). At the same time, recent research on electronic monitoring shows that public sector employees remain highly sensitive to whether such systems are experienced as

developmental or controlling, indicating that governance narratives do not determine meaning unilaterally but are interpreted through lived experience (Miao et al. 2025).

However, trust as a governance logic can also obscure the political dynamics embedded in surveillance (Kritikos and Iphofen 2024). When surveillance practices are presented as neutral or benevolent, they may mask the underlying asymmetries of power and control they operationalise (Introna 2000). Framing surveillance through the discourse of trust can deflect attention from concerns about privacy, managerial overreach, or the normalisation of constant oversight. It can also shift responsibility onto employees, implying that those who reject surveillance are themselves untrustworthy or misaligned with organisational values (Zureik and Salter 2013; Zureike 2003). In this way, trust as a governance logic serves to naturalise surveillance by embedding it within normative claims about fairness, transparency, and accountability. Trust as governance logic therefore has a dual role: as a justifying narrative that sustains organisational authority and as a mechanism that conceals the exercise of control.

Crucially, these two levels of trust are interdependent: interpersonal trust both reflects and shapes governance narratives, while trust as a governance logic, in turn, defines the organisational conditions under which interpersonal trust is built or eroded, rather than emerging solely within isolated dyadic relationships (Perrier et al. 2024).

### **3 Methodology**

This study adopted a qualitative case study approach to explore how surveillance shapes trust within a local government authority. The case study design enabled an in depth investigation of surveillance practices as they are embedded in organisational routines, discourses, and relationships. This facilitated a nuanced understanding of how trust is negotiated across different organisational levels and roles in a digitally monitored environment, with attention to how interpersonal experiences of trust intersect with governance level narratives.

#### *3.1 Research context*

This study focused on a local government authority in the UK, referred to as Council Delta to preserve anonymity. Council Delta is a large-sized local authority that delivers a broad range of services, including housing, education, environmental health, and social care, to a large and socioeconomically mixed resident population. It employs several thousand staff across multiple directorates and administrative levels and is overseen by a corporate leadership team responsible for strategic planning, performance management, and service delivery. In these respects, Council Delta is broadly typical of UK local authorities operating under performance reporting requirements, accountability pressures, and the continuing digitalisation of administrative processes. The council operates through a mix of office-based and hybrid working arrangements. Although much work is undertaken in person, some roles and tasks are carried out partly remotely, making digital systems important for communication, coordination, reporting, and day-to-day oversight.

Council Delta has implemented various surveillance practices augmented with digital technologies that span multiple departments and administrative functions. This includes an enterprise system used to manage workflows, monitor task completion, and generate real time performance data. It also uses an analytics system that aggregates key performance indicators at departmental, team, and individual levels, enabling detailed visibility into workload distribution, attendance patterns, and service response times. In addition, Council Delta utilises the Microsoft Power Platform to monitor workforce performance indicators, enabling visibility into departmental productivity, targets, deadlines, and customer service standards. A series of

Microsoft tools are also used to track internal workflows, including management reporting, and human resource processes.

### *3.2 Data collection*

Data were collected using semistructured interviews, observations, and documentation. This allowed for a rich and contextually grounded understanding of how trust is shaped by surveillance practices within Council Delta. A total of 49 interviews were conducted, comprising 26 managers and 23 employees drawn from a range of departments (Appendix 1). This balance ensured that managerial and employee perspectives were represented, allowing the study to examine how trust was perceived from superordinate and subordinate positions. Participants were purposively selected to capture a breadth of hierarchical roles and departmental affiliations; thereby, ensuring multiple perspectives on trust in a surveillance context were captured. All participants were involved with the council's surveillance practices as the watchers or the watched. Interviews were conducted in person or online, depending on participant preference. The interviews employed a semistructured format, guided by a set of core themes such as performance oversight, workplace visibility, managerial responsibility, and trust. This format offered structure while allowing flexibility to explore unanticipated issues and participant specific experiences. Interviews ranged from 32 to 87 minutes, were audio recorded with consent, and transcribed for analysis.

Observations were conducted in a variety of settings, including staff meetings, formal presentations, and informal employee and managerial interactions. This provided insight into how trust and surveillance were discussed in everyday organisational practices. Observations were documented in a field journal using shorthand notes to capture organisational routines, discursive framings, and interpersonal dynamics. Notes were made after each interview and observation to capture emerging insights and reflections, helping to ensure interpretive consistency. Interview and observational data were complemented by the collection and analysis of internal documents (e.g., strategy papers, implementation guidelines, and technical reports) as well as publicly available materials (e.g., government policies and digital transformation strategies). These sources helped situate the council's surveillance practices within broader sociopolitical narratives and revealed how surveillance was rationalised and institutionally embedded as a governance logic.

All research procedures complied with established ethical standards. Ethical approval was granted by the researcher's university ethics committee before data collection. Informed consent was obtained from Council Delta and all participants, who were assured of their anonymity, the voluntary nature of their involvement, and their right to withdraw at any time. Given the sensitivity of workplace surveillance as a topic, these assurances were reiterated during interviews to encourage open discussion and reduce concerns about possible repercussions. No evidence of self-censorship or reluctance to discuss monitoring practices was identified during the interviews.

### *3.3 Data analysis*

Following Braun and Clarke (2006), the data were analysed thematically, which provided a systematic yet flexible approach for identifying, organising, and interpreting patterns of meaning within the data. Analysis began with a period of familiarisation, during which the researcher reviewed interview transcripts, observational notes, and documentary materials to gain an overall understanding of the content and context. Codes were then generated through a close, line-by-line reading of the transcripts, capturing significant features of the data relevant to surveillance and trust. Although the analysis remained open to unanticipated issues emerging

from the case, it was informed from the outset by sensitising concepts drawn from the literature on interpersonal trust and governance-based understandings of trust. In particular, prior research on trustworthiness, especially ability, benevolence, and integrity, as well as work conceptualising trust as embedded in organisational rules, procedures, and justificatory narratives, informed attention to key patterns within the dataset. Coding was iterative, with earlier codes revisited and refined as later transcripts, observational notes, and documents were analysed and compared. These codes were then reviewed and refined to identify patterns and areas of convergence or tension across participants' accounts. Related codes were collated and grouped into potential themes that captured shared meanings and recurring interpretations, particularly regarding how surveillance was understood as both a managerial tool and a relational experience.

Where extracts spoke to more than one pattern of meaning, they were considered across relevant themes during the review process, with final placement determined by the extract's strongest analytic fit, its contribution to thematic coherence, and its relation to the paper's conceptual focus on interpersonal and governance perspectives of trust. Themes were iteratively reviewed against the coded extracts and the full dataset to ensure coherence and distinctiveness. Throughout this process, interpretation moved back and forth between prior trust scholarship and the empirical material, allowing existing theory to inform analysis while remaining open to insights emerging from the case. Themes were then defined, ensuring that each represented a clear and meaningful aspect of how trust was constructed within Council Delta. These themes were then interpreted in relation to interpersonal and governance logic perspectives of trust, allowing for a dialogue between theory and data. Observational and documentary materials were used to contextualise the interview findings. This analytical process supported a nuanced understanding of how surveillance shapes trust through interconnected social, organisational, and institutional processes.

## **4 Findings**

### *4.1 Interpersonal trust and everyday surveillance encounters*

#### *4.1.1 Surveillance and managerial ability*

Employees' trust in managers was closely tied to how surveillance practices and the data they produced were understood and applied as indicators of managerial competence. Perceptions of ability were not based solely on technical knowledge of the digital systems underpinning surveillance practices, but on how effectively managers interpreted, contextualised, and acted upon the outputs they generated. Trust developed when managers demonstrated the capacity to use digital systems in ways that supported fair and informed decision making. Indeed, several employees described instances where trust in their managers was reinforced because surveillance practices were used to understand workload pressures, identify process inefficiencies, or offer support. These actions signalled that managers possessed the skills and contextual understanding to make competent decisions: *"When a manager can look at the system and see where things are getting stuck, and then actually do something about it, that builds trust. You feel like they've got the skills to help"* (P29). Managers also viewed surveillance generated performance data as a means to support more informed decisions: *"You have to interpret what the system shows. If staff see you can use that information to improve things, they're more likely to trust your decisions"* (P14).

Conversely, trust was undermined when employees felt that managers lacked the ability to interpret surveillance metrics meaningfully. Employees expressed frustration when managers relied too heavily on surface level metrics, such as login times or task completion rates, without considering the broader work context. One employee remarked: *"If your manager doesn't*

*understand your job but judges you based on numbers, it makes you feel like they don't know what they're doing"* (P47). Employees also perceived managerial over reliance on surveillance as a sign of inexperience or avoidance of responsibility: *"If your team leader can't make a call without checking a dashboard, it feels like they don't have the confidence or knowledge to lead properly"* (P37). These contrasting views show how surveillance amplified perceptions of competence. When used diagnostically, it strengthened perceived ability, but when applied mechanically, it signalled managerial inadequacy, eroding trust.

#### *4.1.2 Surveillance and managerial benevolence*

With surveillance practices extending managerial visibility into employees' work, their use was often interpreted as signalling managerial values and motives. When employees believed surveillance was implemented in a considerate, proportionate, and supportive manner, it often built trust by signalling that managers had employees' best interests in mind: *"It's good to know there's a record if something goes wrong or if someone questions what you've done. It makes you feel like your side of the story matters"* (P36). Other employees noted that benevolent managers used surveillance to flag support needs or redistribute workload fairly: *"My manager saw I was overloaded and stepped in to spread out the tasks. That built trust."* (P38). Some managers also framed surveillance as a protective tool for their teams. A manager (P9), for example, was observed referencing performance data to defend a team member against an unfair complaint, explaining that the records demonstrated the employee had followed procedure correctly.

However, employees described a clear distinction between managers who used surveillance to support them and those who used it to micromanage or monitor with suspicion: *"You can tell when it's being used just to keep tabs. If they're constantly checking in, it feels like they don't trust you"* (P48). A manager also acknowledged the risk of surveillance eroding benevolence: *"If the only time staff hear about their performance is when they've done something wrong, they stop trusting the reason for collecting it in the first place"* (P11). Benevolence therefore hinged on intention and communication. Employees who trusted surveillance practices framed them as care or protection, whereas those who distrusted surveillance interpreted the same visibility as suspicion. This duality illustrates how trust was situational and reversible, collapsing quickly when surveillance crossed from supportive to punitive use.

#### *4.1.3 Surveillance and managerial integrity*

Employees assessed managerial trustworthiness based on whether surveillance was applied transparently, used fairly across teams, and aligned with the values communicated by leadership. Trust was reinforced when managers were open about how surveillance would be used and applied it in a consistent and principled way: *"I was told upfront how the reporting tools work, what they track, and why. That matters. It makes it easier to believe what my line manager's doing"* (P41). Some managers also actively worked to build trust by setting clear boundaries around surveillance use: *"I don't use the [analytics] system to micromanage or catch people out... It's about trust, and I try to stick to that"* (P19).

However, employees expressed concern about managers who applied surveillance inconsistently or selectively: *"What really annoys people is when it's used on some teams but not others, or when senior managers are exempt. That makes you question everything"* (P44). Managers echoed this frustration: *"If the rules apply differently depending on who you are, then the entire system loses credibility"* (P8). Other senior managers raised concerns about surveillance practices being introduced without proper explanation or justification. P20 expressed concern that the Microsoft Power Platform used to monitor performance was

introduced without explanation. They noted that several employees appeared uncertain about what data were being collected or why, which created visible discomfort amongst managers. Across these accounts, breaches of integrity, whether through selective use, lack of transparency, or perceived hypocrisy, acted as triggers for cascading distrust that spread from individual managers to Council Delta as a whole.

## 4.2 *Trust as a governance logic in surveillance*

### 4.2.1 *Trust by design: embedding accountability through system features*

Managers frequently described surveillance practices as mechanisms that embedded accountability into everyday processes. These practices were designed to observe and evaluate work through features embedded within digital systems, such as audit trails and performance dashboards. For many managers, these features were seen as offering a form of procedural trust that did not rely on individual relationships, but on the perceived neutrality and reliability of the surveillance infrastructure itself. A director explained: *“The [Microsoft] Power Platform gives us a record of what happened, when, and by whom. That creates a level of trust in the process because it’s not just someone’s word anymore”* (P6). Similarly, a corporate director commented: *“You don’t have to second guess decisions when everything is documented. That clarity builds trust across teams and with the public”* (P25). Employees also recognised how surveillance could protect them from unfair treatment: *“If something goes wrong, I know there’s a record that shows I followed the right steps. That makes me feel safe”* (P47).

Some managers viewed the design of surveillance as creating a shared sense of fairness: *“It’s not just managers checking on staff. We all use the analytics tools and see the same information. That levels the playing field a bit”* (P23). However, other managers were more cautious about over relying on system generated data: *“The tech helps, but you still need to interpret what it shows. You can’t assume the data tells the whole story”* (P14). These reflections suggest that surveillance systems built trust in procedures by institutionalising traceability and shared visibility, yet this same standardisation also displaced interpersonal discretion, subtly redefining what it meant to trust within the council. Despite these reservations, many managers expressed confidence in surveillance practices that were transparent, standardised, and feature rich. These practices were perceived as trustworthy not because of who operated them, but because of how they were designed. By embedding visibility and traceability into everyday activities, surveillance created an environment where trust was structured through technology rather than interpersonal relationships. In this way, trust became a property of the surveillance architecture and logic, providing a form of governance that aligned with organisational demands for transparency, standardisation, and risk management.

### 4.2.2 *Trust as a justificatory narrative*

Managers frequently described how trust was invoked rhetorically to justify the adoption and ongoing use of surveillance. This language served as a justificatory narrative that positioned surveillance not as a form of control, but as a neutral or even supportive practice aligned with values such as transparency, fairness, and accountability. Managers often used trust related language when explaining the rationale behind new surveillance practices: *“We introduce new tools because we want staff to know we’re making decisions based on facts not assumptions”* (P21). Another director framed surveillance as part of a trust based culture: *“We’ve always said that we trust our people to do their jobs. But we also need tools that help us demonstrate that trust is well placed. That’s what the performance data’s for”* (P22). Several managers also drew attention to the use of language in internal communications, policies, and training materials: *“The message we got was that this is about trust and fairness. That these new tools help spot issues early and support staff, not punish them”* (P2). Indeed, Council Delta’s organisational

strategy states that “*We will harness data transparency to build confidence in decision making, ensuring performance monitoring is supportive.*” This reinforces how the language of trust is embedded in formal governance documents.

In contrast, employees viewed this narrative as a strategy to gain compliance or soften the perception of control: “*When they keep repeating ‘this is about trust,’ it makes you question whether that’s really true. It feels like a script*” (P25). In some cases, employees recognised that the idea of trust was being used to align surveillance practices with broader organisational values: “*They want to make it sound like the tools fit with our values. So, they talk about accountability, trust, fairness, and consistency, but whether that’s how it’s experienced is a different matter*” (P41). For others, the repetition of trust related language shaped their expectations and perceptions: “*At first, I was sceptical, but now I see it as normal. It’s part of how they talk about everything here. You just get used to it*” (P45).

This suggests that trust operated not only as an outcome of surveillance but also as a discourse that reframed managerial control as accountability and fairness. While this language helped embed surveillance within organisational norms, its persuasiveness depended on lived experience, revealing the fragility of trust as a rhetorical tool and its potential to mask deeper ambivalences around power and control. This contrast between rhetorical trust and lived mistrust illustrates a process of normalisation. Indeed, the more surveillance was framed as trustworthy, the more employees scrutinised whether it was genuinely fair and consistent in practice, producing a fragile equilibrium between acceptance and scepticism.

#### *4.2.3 Contradictions between trust rhetoric and control practices*

Although surveillance was frequently framed through the language of trust, participants identified tensions between these rhetorical claims and their lived experience of control. Employees and some managers described how technologies were justified as supporting transparency or accountability, while often operating in ways that reinforced managerial oversight, performance pressure, and excessive monitoring. These contradictions called into question whether surveillance genuinely fostered trust or merely presented the appearance of it. Several employees noted how the declared values of trust were inconsistent with how the technologies underpinning surveillance were implemented: “*They say we’re trusted to manage our own work, but then everything’s tracked. It’s hard to feel trusted when you know someone’s always checking your performance*” (P41).

Some managers recognised the difficulty of balancing autonomy with surveillance: “*We encourage staff to take ownership, but our tools are built to escalate anything that looks unusual. That sends a mixed message*” (P17). Other managers described being caught between council expectations and employee interpretations: “*We’re told to build trust with staff. At the same time, we’re asked to report on everyone’s metrics every week. That doesn’t always sit well with staff*” (P2). These contradictions created unease, especially when surveillance was used to enforce compliance rather than to foster improvement: “*They say it’s about learning and support, but I’ve seen people pulled up because of one bad week. That doesn’t build trust*” (P44). These findings indicate that trust eroded not simply because of surveillance itself, but because of a perceived mismatch between espoused values and enacted practices, which generated dissonance among managers and employees.

These accounts illustrate how trust, when positioned as a governance logic, can be undermined when control mechanisms dominate day-to-day experiences. The dissonance between rhetoric and practice reduced the credibility of trust based messaging and, in some cases, amplified

employee scepticism. This highlights the fragility of trust as an organisational value when surveillance fails to reflect the principles they claim to embody.

#### *4.2.4 Trust under strain: when surveillance undermines organisational trust*

Rather than promoting confidence in Council Delta, surveillance eroded trust when it was perceived as inconsistent with core values such as fairness, proportionality, and respect. For some employees and managers, the presence of surveillance did not signal the council's trustworthiness, but its preoccupation with control and suspicion. Employees often expressed concerns about how performance data were collected, interpreted, and acted upon: *"There's never a clear explanation of why certain data is tracked or how it's used. That makes it hard to trust the [enterprise] system or the people behind it"* (P31). A division head echoed this concern during a workshop. They reflected that recent monitoring initiatives seemed misaligned with the council's stated values, noting that some staff appeared more conscious of being watched than supported during discussions of performance targets. Trust was also undermined when surveillance clashed with expectations of fairness: *"Sometimes it feels like certain people are being watched more closely than others. That creates resentment and damages trust in the whole thing"* (P42). A director also highlighted the risk of losing moral credibility: *"Once staff believe that performance monitoring is about control rather than support, it becomes very hard to convince them otherwise"* (P6).

These examples reveal a key mechanism of the fragility of trust. Once surveillance breaches perceived boundaries, its effects radiate beyond the individual to the organisational level, undermining confidence in the council's integrity. Indeed, when surveillance is perceived as misused or overreaching, it not only fails to foster trust but also actively contributes to its erosion. Rather than reinforcing a sense of shared organisational purpose, surveillance prompts employees and some managers to question the council's trustworthiness and ethical foundations. In this way, trust in surveillance is not inherent in its design, but contingent on how it is perceived and experienced by those affected. Viewed alongside interpersonal experiences, these governance logics both enable and conflict with lived practice, producing frictions that unsettle the promise of surveillance based trust.

## **5 Discussion**

This study contributes to the literature on trust and surveillance by developing an integrated multilevel account that brings together interpersonal and governance perspectives. While prior studies tend to treat these levels separately (e.g., Schweitzer, Ho, and Zhang 2018; Bijlsma-Frankema, de Jong, and de Bunt 2008; Westin 1992; Alge and Hansen 2014; Flatøy and Lund-Tønnesen 2025; Perrier et al. 2024), and recent review work suggests that the effects of electronic monitoring are often contingent rather than uniform (König 2025), the analysis here demonstrates how their interaction produces tensions that render trust fragile and contested. This extends Mayer et al.'s (1995) model by situating interpersonal trust within broader governance logics, showing how organisational narratives of fairness and accountability reshape everyday trust relations in a local government authority. It further reveals a recursive dynamic, whereby governance narratives influence interpersonal interpretations of surveillance, while employees' experiences feed back into and challenge these governance logics. In this respect, the study resonates with research that highlights the multilevel character of trust within public sector organisations (Perrier et al. 2024). The study also responds to calls for research applying a digital surveillance governance perspective to better understand the changes occurring in the public sector and how they are experienced and negotiated through trust (Lund-Tønnesen 2026).

### *5.1 Foregrounding interpersonal trust in surveillance*

This study reveals how surveillance shapes interpersonal trust through employee perceptions of managerial ability, benevolence, and integrity in complex and sometimes contradictory ways. Surveillance reinforces employee perceptions of ability when managers use performance data effectively, make informed decisions, and intervene in a timely and competent manner to support service delivery. This strengthens employee confidence in managerial judgement and competence. However, when managers misinterpret data, delay interventions, or rely on metrics without understanding context, employee perceptions of ability are undermined. The visibility that surveillance affords can therefore expose managerial shortcomings, which erode trust rather than reinforce it.

This insight extends existing theorisations, which often assume surveillance simply signals managerial mistrust (Zureike 2003; Holland, Cooper, and Hecker 2015; König 2025). Indeed, by showing how perceptions of managerial ability can be both confirmed and destabilised through surveillance, this study moves beyond oppositional framings of ‘trust versus control’ (e.g., Bijlsma-Frankema, de Jong, and de Bunt 2008; Ball 2010; Tække 2011; Abendroth, Schröder, and Meyer 2026). It instead reveals how managerial ability is continuously evaluated in surveilled environments, where every data driven decision contributes to the fragile construction of trust (Klöpper and Rowe 2026). Small errors in interpretation or action can quickly erode the confidence that surveillance was meant to enhance. This fragility is particularly salient in the public sector, where digital technologies make managerial decisions highly visible in the name of transparency and accountability (Webster 2012; Viola and Laidler 2022; Miao et al. 2025).

Similarly, benevolence as a dimension of trust is reinforced when managers use surveillance to protect employees, distribute workload fairly, eliminate favouritism, and resolve disputes. In these situations, surveillance is not viewed as punitive but as a practice through which managerial care and concern are enacted. However, when managers are perceived as using surveillance to apportion blame, micromanage, or ignore staff well-being, it can quickly become a source of anxiety, signalling that control is being prioritised over support. While previous studies acknowledge that surveillance damages employee trust (Bernstrøm and Svare 2017; Holland, Cooper, and Hecker 2015; Alge and Hansen 2014; Abendroth, Schröder, and Meyer 2026), this study advances that debate by showing how benevolence can be enacted or denied through surveillance practices mediated by digital technology. This also complements public sector research showing how employees respond differently to monitoring depending on whether it is experienced as developmental or controlling (Miao et al. 2025).

This study thus advances debates on trust by showing how perceptions of managerial benevolence are increasingly mediated through surveillance, where the way data are used (or ignored) become a proxy for managerial intent. In doing so, the study contributes to a more granular understanding of how trust is constructed through digital encounters, rather than solely through face-to-face interactions (Schweitzer, Ho, and Zhang 2018). Yet these findings also highlight contradictions because the same surveillance practices that allow managers to demonstrate care can equally be read as instruments of suspicion, making trust contingent, fragile, and easily reversed (Miao et al. 2025). It also provides insight into how these dynamics play out in the public sector, where employee expectations of fairness and support are often linked to institutional missions of equity and care (Webster 2012; Kayas et al. 2019). This points to a deeper instability, where interpersonal trust is not only fragile but persistently contested in employees’ interpretations, where identical surveillance practices can be seen as caring or coercive depending on relational climate (Sewell and Barker 2006).

Integrity as a dimension of trust is shown to depend on employees' perceptions of the consistency, transparency, and fairness with which surveillance is deployed. When surveillance practices are aligned with organisational values and applied equitably across teams, they are more likely to be interpreted as expressions of managerial honesty and ethical conduct. However, when surveillance practices are perceived as intrusive, selectively applied, or inconsistent with stated principles, trust in managerial integrity is damaged. This insight addresses a notable shortcoming in existing research, which tends to overlook how trust is undermined not only by the presence of surveillance, but by its procedural and moral inconsistencies (Alge and Hansen 2014; Chory, Vela, and Avtgis 2016). This advances the theoretical debate by showing how employee assessments of integrity are shaped by both interpersonal interactions and perceived organisational ethics. In doing so, this study produces a novel multilevel perspective on trust, explaining why some surveillance practices are experienced as caring while others are seen as coercive or manipulative (Sewell and Barker 2006).

The findings also extend quantitative research suggesting that employee perceptions of management's trust in them are relatively robust to monitoring in public sector settings, even when monitoring shapes turnover intention (Flatøy and Lund-Tønnesen 2025). By examining these dynamics qualitatively within a local government authority, this study shows that such apparent robustness can coexist with more fragile and contested dynamics in practice, as employees continually reinterpret surveillance through everyday judgements about fairness, support, and control. This difference may partly reflect context. Indeed, Flatøy and Lund-Tønnesen's Norwegian study examines monitoring in a high-trust societal setting, whereas this study shows how trust can remain vulnerable to the local meanings employees attach to fairness, support, and control within a specific UK public authority. Such patterns are also unlikely to be distributed evenly, given evidence that employee jobs in more resource-rich organisations can be shielded from more invasive forms of digital monitoring (Abendroth, Schröder, and Meyer 2026).

The analysis further demonstrates that interpersonal trust is actively built, undermined, and renegotiated through everyday encounters with surveillance. Trust in managers can be reinforced when surveillance is fair, proportionate, and aligned with professional values (Alge and Hansen 2014), but it remains unstable because small breaches of ability, benevolence, or integrity can undermine it quickly. Its fragility reflects how surveillance amplifies everyday vulnerabilities in the employee–manager relationship, leaving trust continuously open to contestation. Interpersonal trust within surveillance environments is therefore simultaneously fragile and contested. It is fragile because it is easily established and undone through daily managerial actions. At the same time, it is contested because employees continually reinterpret surveillance through competing meanings of care, control, and fairness. This underscores the multilevel nature of trust in surveillance, where vulnerability and evaluation are constant features of organisational life. These interpersonal dynamics also act as feedback mechanisms that reinforce or challenge the broader governance logics framing surveillance, linking everyday sense making with institutional trustworthiness.

## *5.2 Framing trust as governance logic in surveillance*

This study produces new insight by showing how surveillance practices are presented as tools of trust rather than control, both in their design and in the narratives used to justify them. It reveals that trust is not only an interpersonal relation but also a symbolic and structural component of surveillance governance. Across the findings, trust was embedded into digital

architectures through accountability features, invoked rhetorically to justify surveillance practices, and undermined when the council's messaging of trust contradicted how employees experienced surveillance. This elucidates how trust in surveillance governance is deeply contradictory and fragile, functioning simultaneously as a technical property, a rhetorical resource, and a site of contestation. Here, fragility reflects how trust as a governance logic unravels when surveillance practices diverge from organisational values. Simultaneously, contestation captures how employees actively challenge and reinterpret organisational claims that surveillance is trustworthy. These dynamics were pronounced in Council Delta, where institutional expectations of transparency and fairness heightened the visibility and stakes of surveillance (Bowman and West 2021; Hood 2007; Viola and Laidler 2022). In doing so, the study builds on Lund-Tønnesen's (2026) account of digital surveillance governance by showing how public sector dynamics of control, transparency, and data-driven oversight are enacted and contested at the organisational level through trust-laden narratives that seek to reconcile surveillance with fairness and support.

Through the concept of trust as governance logic, this paper further shows that surveillance practices can be understood as part of a multilevel account in which trust serves not as a stable organising principle but as a fragile and contested mechanism of organisational justification. Indeed, accountability features such as audit trails, access logs, and dashboards are positioned as trust enhancing mechanisms, suggesting that transparency and traceability are substitutes for interpersonal confidence (Power 1997). Yet, this instrumentalisation of trust frequently masks underlying contradictions. While surveillance is rhetorically framed as evidence of trust in employees' professionalism, its introduction often extends managerial oversight and reinforces hierarchical control (Kayas 2023; Kayas et al. 2019). In public sector contexts, where surveillance is increasingly aligned with demands for auditability and due process (Kayas et al. 2019; Charbonneau and Doberstein 2020; Webster 2012; Flatøy and Lund-Tønnesen 2025; Perrier et al. 2024), this tension is amplified by the need to simultaneously demonstrate both managerial control and moral credibility.

In this way, the study unveils the symbolic work that trust performs in justifying surveillance. Rather than dismissing such narratives as organisational hypocrisy (Weckert 2000), trust operates as a mode of organisational sensemaking, bridging tensions between control and empowerment, and between transparency and suspicion. Yet these narratives are precarious. Indeed, this study shows that when surveillance contradicts rhetorical commitments to fairness or proportionality, trust quickly unravels, exposing the contradictions at the heart of governance logics. In this sense, trust as governance logic is not only fragile but actively contested, as institutional narratives of transparency and accountability collide with employees' lived experiences of oversight. This was particularly relevant in Council Delta, where the justification of surveillance must navigate internal expectations of procedural fairness and external pressures for political accountability (Charbonneau and Doberstein 2020; Kayas et al. 2019; Bowman and West 2021). At the governance level too, trust emerges as both fragile and contested. While it is fragile because its trustworthiness depends on consistent alignment between rhetoric and practice, it is contested because employees resist or reinterpret the institutional narratives that seek to define surveillance as trustworthy. Together, these dynamics contribute by highlighting how trust is continuously negotiated across both interpersonal and governance levels, rather than secured through design or discourse.

## **6 Conclusion**

This paper examined how workplace surveillance shapes trust by analysing it from both interpersonal and governance levels. It contributes by extending existing theorisations of trust's

fragility through a multilevel account that shows how trust depends on the alignment between interpersonal and governance experiences of surveillance. Trust's fragility arises from the tensions between these levels in public organisations utilising surveillance practices mediated by digital technology. The study reveals how employee perceptions of managerial ability, benevolence, and integrity can both strengthen and undermine interpersonal trust through the use of surveillance, and shape trust as a governance logic through the design, justifying narratives, and organisational practices of surveillance. Crucially, these two levels intersect in ways that generate tensions, contradictions, and misalignments, resulting in trust that is neither stable nor uniform but continually negotiated and fragile. At the interpersonal level, trust is built or eroded through everyday encounters with surveillance. However, at the governance level, it is invoked rhetorically to justify surveillance, yet is frequently challenged in practice. This multilevel perspective advances research beyond binary framings of 'trust versus control' and single level analyses, demonstrating instead how surveillance simultaneously builds, erodes, and justifies trust. Situated within the value laden context of a local government authority, the analysis highlights the complex ways in which surveillance shapes organisational trustworthiness and employee–manager relations.

Although this study offers valuable insight into trust in surveillance, it has limitations that offer avenues for future research. First, the analysis foregrounds Mayer et al.'s (1995) model of trust. While useful, it may not fully capture other relational or institutional dimensions. Future studies could therefore integrate alternative trust frameworks, such as the model of trust development by Lewicki and Bunker (1996), which distinguishes between calculus based, knowledge based, and identification based trust to examine how each evolves in surveillance contexts. Second, this study focused on employees and managers, omitting perspectives from government officials, policymakers, or technology vendors, who could reveal additional forces shaping how trust and surveillance are shaped, justified, and experienced.

## 7 References

- Abendroth, Anja-Kristin, Charlotte Katharina Schröder, and Sophie-Charlotte Meyer. 2026. The Social Structuring of Digital Monitoring: How Resource-Rich Employees Are Shielded from More Invasive Levels of Digital Monitoring. *New Technology, Work and Employment*. <https://doi.org/10.1111/ntwe.70019>.
- Alder, G S, T W Noel, and M L Ambrose. 2006. Clarifying the Effects of Internet Monitoring on Job Attitudes: The Mediating Role of Employee Trust. *Information & Management* 43 (7): 894–903. <https://doi.org/10.1016/j.im.2006.08.008>.
- Alge, Bradley J, and Duane S Hansen. 2014. Workplace Monitoring and Surveillance Research since "1984": A Review and Agenda. In *The Psychology of Workplace Technology*, edited by Michael D Coovert and Lori Foster Thompson, 209–237. East Sussex: Routledge.
- Ball, Kirstie. 2003. Editorial. The Labours of Surveillance. *Surveillance & Society* 1 (2): 125–137.
- Ball, Kirstie. 2010. Workplace Surveillance: An Overview. *Labor History* 51 (1): 87–106. <https://doi.org/10.1080/00236561003654776>.
- Ball, Kirstie. 2021. *Electronic Monitoring and Surveillance in the Workplace: Literature Review and Policy Recommendations*. Joint Research Centre (Luxembourg: Publications Office of the European Union).
- Ball, Kirstie. 2022. Surveillance in the Workplace: Past, Present, and Future. *Surveillance & Society* 20 (4): 455–461. <https://doi.org/10.24908/ss.v20i4.15805>.

- Bentzen, Tina Øllgaard, Marte Winsvold, and Frédérique Six. 2026. Beyond the Birdcage: Building Trust in Different Regulatory Contexts. *Public Management Review*: 1–27. <https://doi.org/14719037.2026.2623188>.
- Bernstrøm, Vilde Hoff, and Helge Svare. 2017. Significance of Monitoring and Control for Employees' Felt Trust, Motivation, and Mastery. *Nordic Journal of Working Life Studies* 7 (4): 29–49. <https://doi.org/10.18291/njwls.v7i4.102356>.
- Bijlsma-Frankema, K., B. de Jong, and G. V. de Bunt. 2008. Heed, a Missing Link between Trust, Monitoring and Performance in Knowledge Intensive Teams. *International Journal of Human Resource Management* 19 (1): 19–40. <https://doi.org/10.1080/09585190701763800>.
- Bowman, James S, and Jonathan P West. 2021. *Public Service Ethics*. 3 ed. New York: Routledge.
- Braun, Virginia, and Victoria Clarke. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 32 (2): 77–101. <https://doi.org/10.1191/1478088706qp063oa>.
- Charbonneau, E, and C Doberstein. 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, Chung-An, Chih-Wei Hsieh, and Dong-Yun Chen. 2014. Fostering Public Service Motivation through Workplace Trust: Evidence from Public Managers in Taiwan. *Public Administration* 92 (4): 954–973. <https://doi.org/10.1111/padm.12042>.
- Chory, Rebecca M, Lori E Vela, and Theodore A Avtgis. 2016. Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses. *Employee Responsibilities and Rights Journal* 28: 23–43. <https://doi.org/10.1007/s10672-015-9267-4>.
- Diefenbach, Thomas. 2009. New Public Management in Public Sector Organizations: The Dark Sides of Managerialistic 'Enlightenment'. *Public Administration* 87 (4): 892–909. <https://doi.org/10.1111/j.1467-9299.2009.01766.x>.
- Dirks, Kurt T, and Donald L Ferrin. 2001. The Role of Trust in Organizational Settings. *Organization Science* 12 (4): 393–521. <https://doi.org/10.1287/orsc.12.4.450.10640>.
- Ferry, Laurence, and Henry Midgley. 2024. Are Public Sector Accounts Trusted? Exploring the Verdict of the Public Administration and Constitutional Affairs Committee in the United Kingdom. *Public Administration* 102 (4): 1450–1467. <https://doi.org/10.1111/padm.12983>.
- Flatøy, Christer A, and Jonas Lund-Tønnesen. 2025. Electronic Monitoring, Trust, and Turnover Intention in the Public and Private Sector. *Public Management Review*: 1–28. <https://doi.org/10.1080/14719037.2025.2608281>.
- Giddens, Anthony. 1990. *The Consequences of Modernity*. Cambridge: Polity Press.
- Giddens, Anthony. 2013. *The Consequences of Modernity*. Cambridge: Polity Press.
- Gilliom, John, and Torin Monahan. 2013. *Supervision*. Chicago: University of Chicago Press.
- Glavin, Paul, Alex Bierman, and Scott Schieman. 2024. Private Eyes, They See Your Every Move: Workplace Surveillance and Worker Well-Being. *Social Currents* 11 (4). <https://doi.org/10.1177/23294965241228874>.
- Gulati, Ranjay, and Jack A Nickerson. 2008. Interorganizational Trust, Governance Choice, and Exchange Performance. *Organization Science* 19 (5): 669–806. <https://doi.org/10.1287/orsc.1070.0345>.
- Hillo, Jaakko, Isak Vento, and Tero Erkkilä. 2025. Algorithmic Governance: Experimental Evidence on Citizens' and Public Administrators' Legitimacy Perceptions of Automated Decision-Making. *Public Administration*. <https://doi.org/10.1111/padm.70028>.

- Holland, Peter Jeffrey, Brian Cooper, and Rob Hecker. 2015. Electronic Monitoring and Surveillance in the Workplace: The Effects on Trust in Management, and the Moderating Role of Occupational Type. *Personnel Review* 44 (1): 161–175. <https://doi.org/10.1108/PR-11-2013-0211>.
- Hood, Christopher. 2007. Public Service Management by Numbers: Why Does It Vary? Where Has It Come From? What Are the Gaps and the Puzzles? *Public Money & Management* 27 (2): 95–102. <https://doi.org/10.1111/j.1467-9302.2007.00564.x>.
- Introna, Lucas D. 2000. Workplace Surveillance, Privacy, and Distributive Justice. *Computers and Society*. <https://doi.org/10.1145/572260.572267>.
- Introna, Lucas D. 2003. Opinion. Workplace Surveillance ‘Is’ Unethical and Unfair. *Surveillance & Society* 1 (2): 210–216. <https://doi.org/10.24908/ss.v1i2.3354>.
- Kayas, Oliver George. 2023. Workplace Surveillance: A Systematic Review, Integrative Framework, and Research Agenda. *Journal of Business Research* 168: 114212. <https://doi.org/10.1016/j.jbusres.2023.114212>.
- Kayas, Oliver George, Eang Ong Chin, and H M Belal. 2025. From Humans to Algorithms: A Sociotechnical Framework of Workplace Surveillance. *Digital Business* (100120). <https://doi.org/10.1016/j.digbus.2025.100120>.
- Kayas, Oliver George, Tony Hines, Rachel McLean, and Gillian H Wright. 2019. Resisting Government Rendered Surveillance in a Local Authority. *Public Management Review* 21 (8): 1170–1190. <https://doi.org/10.1080/14719037.2018.1544661>.
- Klöpffer, Miriam, and Frantz Rowe. 2026. People Analytics, Trust Erosion and Intention to Leave: The Role of Information Asymmetry. *Information & Management* 63 (4): 104346. <https://doi.org/10.1016/j.im.2026.104346>.
- König, Cornelius J. 2025. Electronic Monitoring at Work. *Annual Review of Organizational Psychology and Organizational Behavior* 12: 321–342. <https://doi.org/10.1146/annurev-orgpsych-110622-060758>.
- Kritikos, Mihalis, and Ron Iphofen. 2024. Develop a Workplace/Employee-Specific Data Governance Strategy That Strengthens the Rights to Privacy and Data Protection in the Digital Workplace. In *Ethical Ai Surveillance in the Workplace: Ethical, Legal, and Governance Issues*, edited by Mihalis Kritikos and Ron Iphofen. Leeds: Emerald Publishing Limited.
- Li, Jiayuan. 2015. The Paradox of Performance Regimes: Strategic Responses to Target Regimes in Chinese Local Government. *Public Administration* 93 (4): 1152–1167. <https://doi.org/10.1111/padm.12197>.
- Lund-Tønnesen, Jonas. 2026. Digital Surveillance Governance: Understanding Developments in the Use of Personal Data in Public Sector Reform. *Public Management Review*. <https://doi.org/10.1080/14719037.2026.2620546>.
- Mayer, Roger C, James H Davis, and F David Schoorman. 1995. An Integrative Model of Organizational Trust. *The Academy of Management Review* 20 (3): 709–734.
- McAllister, Daniel J. 1995. Affect-and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations. *Academy of Management Journal* 38 (1): 24–59. <https://doi.org/10.5465/256727>.
- Mettler, Tobias. 2024. 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>.
- Miao, Qing, Hui Yind, Gary Schwarz, and Muhammad Ali Hussain. 2025. Disentangling the Impact of Perceived Electronic Performance Monitoring on Employee Burnout in the Public Sector. *Public Management Review* 27 (12): 3028–3056. <https://doi.org/10.1080/14719037.2024.2396080>.

- Morales, Fernando Nieto, Rafael Wittek, and Liesbet Heyse. 2015. Organizational Pathways to Compliant Reform Implementation: Evidence from Mexican Civil Service Reform. *Public Administration* 93 (3): 646–662. <https://doi.org/10.1111/padm.12157>.
- Natan-Krup, Dana, and Shlomo Mizrahi. 2025. Public Accountability and Auditing: Why and When Do State Auditors Conduct Broad Audits? *Public Administration* 103 (1): 166–184. <https://doi.org/10.1111/padm.13012>.
- Pan, Chao, Tingting Song, and Zheng Jiang. 2026. Trapped in the Digital Net: The Consequences of Electronic Monitoring and Digital Overload for Civil Servants. *Public Performance & Management Review*. <https://doi.org/10.1080/15309576.2026.2632947>.
- Perrier, Anthony, Assâad El Akremi, Caroline Manville, and Mathieu Molines. 2024. “It's All About Trust!” a Multilevel Model of the Effect of Servant Leadership on Firefighters' Group Task Performance, Adaptivity and Emotional Exhaustion. *Public Administration Review* 85 (4): 1150–1172. <https://doi.org/10.1111/puar.13893>.
- Power, Michael. 1997. *The Audit Society: Rituals of Verification*. Oxford: Oxford University Press.
- Rychwalska, Agnieszka, Goodell Geoffrey, and Magdalena Roszczynska-Kurasinska. 2021. Data Management for Platform-Mediated Public Services: Challenges and Best Practices. *Surveillance & Society* 19 (1): 22–36. <https://doi.org/10.24908/ss.v19i1.13986>.
- Schweitzer, M. E., T. H. Ho, and X. Zhang. 2018. How Monitoring Influences Trust: A Tale of Two Faces. *Management Science* 64 (1): 253–270. <https://doi.org/10.1287/mnsc.2016.2586>.
- Sewell, Graham, and James R Barker. 2006. Coercion Versus Care: Using Irony to Make Sense of Organizational Surveillance. *Academy of Management Review* 31 (4): 934–961.
- Soomro, Shuaib Ahmed, Faisal Qamar, Slim Hadoussa, and Yasir Mansoor Kundi. 2025. Digital Transformation and Electronic Performance: Exploring the Relationship between Fairness Perception, Organizational Identification, and Individual Performance. *Review of Managerial Science* 19: 1297–1316. <https://doi.org/10.1007/s11846-024-00792-8>.
- Tække, J. 2011. Digital Panopticism and Organizational Power. *Surveillance & Society* 8 (4): 441–454. <https://doi.org/10.24908/ss.v8i4.4181>.  
<https://www.scopus.com/inward/record.uri?eid=2-s2.0-84864738205&doi=10.24908%2fss.v8i4.4181&partnerID=40&md5=17d5007a13f10457c6d6e5aa603c91fe>  
<https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/download/4181/4183>.
- Thornton, Patricia H, William Ocasio, and Michael Lounsbury. 2012. *The Institutional Logics Perspective: A New Approach to Culture, Structure, and Process*. Oxford: Oxford University Publishing.
- Viola, Lora Anne, and Paweł Laidler. 2022. On the Relationship between Trust, Transparency and Surveillance. In *Routledge Studies in Surveillance: Trust and Transparency in an Age of Surveillance*, edited by Lora Anne Viola and Paweł Laidler, 3–18. Oxon: Routledge.
- Webster, C William, R. 2012. Public Administration as Surveillance. In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin Haggerty and David Lyon, 313–320. London: Routledge.
- Weckert, John. 2000. Trust and Monitoring in the Workplace. IEEE International Symposium on Technology and Society, Rome, Italy, 8 September 2000.
- 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](https://doi.org/10.1016/0003-6870(92)90008-J).

Zureik, Elia, and Mark Salter. 2013. Global Surveillance and Policing: Borders, Security, Identity - Introduction. In *Global Surveillance and Policing: Borders, Security, Identity*, edited by Elia Zureik and Mark Salter, 1–10. London: Taylor & Francis.

Zureike, Elia. 2003. Theorizing Surveillance: The Case of the Workplace. In *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, edited by David Lyon, 31–56. London: Routledge.

## Appendix 1: participant details

Managers		
Participant ID	Role	Department/Function
P1	Division Head	Social Care
P2	Team Leader	Customer Services
P3	Corporate Director	Communications & Marketing
P4	Lead	Communications & Marketing
P5	Team Leader	Social Care
P6	Director	Transport & Environment
P7	Division Head	Tourism
P8	Team Leader	Communications & Marketing
P9	Team Leader	Human Resources
P10	Head of Services	Digital Systems
P11	Lead	Social Care
P12	Lead	Human Resources
P13	Team Leader	Executive Branch
P14	Head of Services	Tourism
P15	Team Leader	Communications & Marketing
P16	Division Head	Estates
P17	Division Head	Digital Systems
P18	Head of Services	Highways
P19	Director	Highways
P20	Senior Executive	Finance
P21	Senior Executive	Estates
P22	Director	Finance
P23	Team Leader	Highways
P24	Director	Governance
P25	Corporate Director	Highways
P26	Team Leader	Finance
Employees		
P27	Housing Officer	Housing Services
P28	Customer Service Advisor	Customer Services
P29	Support Worker	Social Care
P30	Environmental Health Officer	Environmental Health
P31	Education Welfare Officer	Education
P32	HR Administrator	Human Resources
P33	Transport Coordinator	Transport
P34	Finance Officer	Finance

<b>P35</b>	Democratic Services Officer	Governance
<b>P36</b>	Property Maintenance Technician	Estates
<b>P37</b>	Visitor Information Assistant	Tourism
<b>P38</b>	Communications Assistant	Communications & Marketing
<b>P39</b>	Waste Collection Operative	Waste Management
<b>P40</b>	Care Support Assistant	Adult Services
<b>P41</b>	Community Engagement Officer	Community Development
<b>P42</b>	IT Support Technician	Digital Services
<b>P43</b>	Library Assistant	Libraries
<b>P44</b>	Planning Officer	Planning
<b>P45</b>	Benefits Assessment Worker	Revenues and Benefits
<b>P46</b>	Public Health Advisor	Public Health
<b>P47</b>	Family Support Worker	Children's Services
<b>P48</b>	Legal Assistant	Legal Services
<b>P49</b>	Grounds Maintenance Operative	Parks and Recreation