Government Information Quarterly 43 (2026) 102162

Contents lists available at ScienceDirect

Government Information Quarterly

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

Managerial resistance to digital workplace surveillance in a local government authority

Oliver George Kayas [a,*], Efpraxia D. Zamani [b]

[a] Liverpool John Moores University, Liverpool Business School, Brownlow Hill, Liverpool, L3 5UG, UK
[b] University of Durham, Durham Business School, Waterside, Durham DH1 1SL, UK

ARTICLE INFO

Keywords:
Workplace surveillance
Management resistance
Digital technology
Sociotechnical systems
Public service ethics
Local government

ABSTRACT

Workplace surveillance is an increasingly pervasive feature of contemporary organisations, yet research overwhelmingly positions employees as its primary subjects and agents of resistance. Managers, by contrast, are implicitly framed as a homogeneous group who design, implement, and sustain surveillance. We argue that such framing ignores the complex positions managers simultaneously occupy as implementers, mediators, and potential subjects of surveillance, and further obscures situations in which they themselves are monitored, oppose surveillance, or actively engage in resisting it. Drawing on a grounded theory study of a UK local government authority, we examine how and why managers resist digitally augmented surveillance systems, revealing three interrelated resistance strategies: shielding employees from surveillance, obfuscating data to undermine system integrity, and deploying discursive practices to contest surveillance legitimacy. These strategies are simultaneously shaped by self-protective and value-driven motivations. By integrating sociotechnical systems theory with public service ethics, we develop a conceptual framework that repositions managers as agentive, morally reasoning actors navigating the contested terrain of digital control. The findings advance interdisciplinary understanding of resistance and ethics in digitally mediated public sector organisations, and respond to calls for research that recognises managerial diversity and conceptualises resistance as a situated sociotechnical process.

1. Introduction

Workplace surveillance is an increasingly pervasive feature of contemporary organisations, driven by performance goals and the proliferation of digital technologies that enable the automated collection and analysis of workforce data (Kayas, Chin, & Belal, 2025). Public sector organisations are no exception to the widespread adoption of digital surveillance systems. Enterprise systems, performance management systems, data analytics, dashboards, and reporting systems, for example, provide public sector organisations with surveillance infrastructures, by embedding managerial oversight into performance controls and metrics that structure and monitor the work of subordinates through technological mediation (Afzal & Panagiotopoulos, 2024; AlGhamdi, Win, & Vlahu-Gjorgievska, 2022; Janssen, Brous, Estevez, Barbosa, & Janowski, 2020).

These surveillance systems create tensions around autonomy, trust, and ethical responsibility, where professional discretion, service values, transparency, and accountability are central (Kayas, Hines, McLean, & Wright, 2019; Roztocki, Strzelczyk, & Weistroffer, 2025). Local government authorities, in particular, must navigate complex tensions between surveillance and the values of care, equity, and professional integrity, while working under conditions of public accountability, procedural scrutiny, and service responsibility (Schubad, Bernards, van der Pas, & Groeneveld, 2026). Although attention has been paid to how employees contest these tensions (e.g., Charbonneau & Doberstein, 2020; Kayas et al., 2019), little is known about the complex positions that managers occupy: operating simultaneously as implementers, mediators, and potential subjects of surveillance (Ball, 2021; Kayas, 2023).

Despite multiple calls, research overwhelmingly positions employees as the primary subjects of surveillance and the central agents of resistance (Ball, 2021; Kayas, 2023). At the same time, managers are implicitly framed as a homogeneous group who design, implement, operate, and sustain surveillance (e.g., Clawson & Clawson, 2017). Such studies ignore differences in managerial responsibilities, authority, values, and ethical views toward surveillance. They also fail to address situations in which managers themselves are monitored or ethically opposed to surveillance, thereby overlooking them as active agents who resist surveillance.

* Corresponding author at: Liverpool John Moores University, Liverpool Business School, Brownlow Hill, Liverpool L3 5UG, UK.
E-mail addresses: o.g.kayas@ljmu.ac.uk (O.G. Kayas), efpraxia.zamani@durham.ac.uk (E.D. Zamani).

https://doi.org/10.1016/j.giq.2026.102162
Received 2 December 2025; Received in revised form 1 June 2026; Accepted 5 June 2026
Available online 13 June 2026

As a result, research is yet to explore how managerial responses to surveillance shape who is targeted, the underlying conditions, and the mode (e.g., collective, covert) of managers' resistance. Without this understanding, research risks neglecting the specific types of managerial resistance enacted and the conditions under which this may be possible. Furthermore, most resistance to surveillance research focuses on obstructive approaches (Kayas, 2023), overlooking forms of productive resistance that may benefit the organisation and its members (Courpasson, Dany, & Clegg, 2011). This leaves a significant theoretical gap relating to how obstructive and productive managerial resistance emerges through the interaction of sociotechnical surveillance systems, organisational hierarchies, and ethical commitments. This is especially important for local government authorities where accountability, care, integrity, transparency, fairness, and public service ethics are paramount (Misra, Katz, Roberts, Carney, & Valdivia, 2024; Saldanha, Dias, & Guillaumon, 2022).

To address this, we ask: How and why do managers resist surveillance systems augmented with digital technology within a local government authority? Drawing on 26 semi-structured interviews with managers, observations, and documentary materials from a UK local government authority, we adopted a grounded theory methodology to examine managers' experiences, interpretations, and resistance activities in relation to workplace surveillance. This approach enabled patterns and relationships to be developed from managers' accounts, allowing us to explain how and why resistance emerges in local government. The analysis subsequently develops a conceptual framework of managerial resistance in a local government context, which was further refined through engagement with existing literature on surveillance (e.g., Ball, 2010; Sewell & Barker, 2006), resistance (Ball, 2010; Krishnan & Krishnan, 2025; Valtonen & Holopainen, 2025), sociotechnical systems (e.g., Alshallaqi, 2024; Avgerou & McGrath, 2007; Ball, 2002; Tangi, Müller, & Janssen, 2025), and public service ethics (e.g., Demmkea, Autioniemi, & Lenner, 2025; Ifenthaler & Tracey, 2016; Natan-Krup & Mizrahi, 2025). This enables a contextually grounded understanding of the motivations, types, and outcomes of managerial resistance, revealing how resistance emerges in a local government authority through the interaction of social, technical, organisational, and ethical factors. By generating theory from managerial experiences, the study responds to calls for research that recognises the diversity of managerial roles in surveillance systems and conceptualises resistance as a situated, sociotechnical process rather than an employee-focused phenomenon (Ball, 2021; Ball & Margulis, 2011; Kayas et al., 2019; Kayas et al., 2025).

We begin by outlining workplace surveillance and managerial resistance to surveillance. Following this, we describe the grounded theory methodology used in the study. The findings are then presented, and we develop a conceptual framework of managerial resistance to workplace surveillance. The theoretical and practical implications of the study are subsequently discussed. We conclude by summarising the contributions, limitations, and opportunities for future research.

2. Literature review

2.1. Workplace surveillance

Workplace surveillance involves augmenting organisational control processes with digital technologies to purposefully observe and evaluate data on employee behaviours, performance, and personal characteristics (Ball, 2010). Accordingly, surveillance not only involves technology-mediated observations, but also symbolic processes embedded in organisational practices and systems (Ball & Margulis, 2011; Sewell & Barker, 2006). Workplace surveillance can thus be conceptualised as a sociotechnical system shaped by technologies, organisational culture, social processes, management ideologies, and diverse organisational actors (Ball, 2002; Kayas et al., 2025). From a sociotechnical perspective (Avgerou & McGrath, 2007; Tangi et al., 2025), surveillance is therefore understood as a dynamic configuration of monitoring wherein technology and social context continually shape one another (Alshallaqi, 2024; Kayas et al., 2025). Within this perspective, sociotechnical affordances are the action possibilities that arise from the interaction between technological features and organisational arrangements, becoming consequential through how actors enact, interpret, and negotiate them in practice (Leonardi, 2011).

Indeed, research suggests that digital work systems should be understood as co-evolving arrangements in which technologies, work practices, and organisational structures adapt together over time, rather than remaining stable once implemented (Parker et al., 2025). This is especially relevant where AI-enabled and data-intensive systems generate opaque inferences and informational asymmetries that reshape autonomy, oversight, and accountability at work (Carter, 2025). The different technologies underpinning surveillance systems may therefore invite different responses because they vary in the visibility, persistence, granularity, and contestability they create, as well as the degree of interpretive flexibility available to organisational actors (Kayas et al., 2025). Dashboards, performance trackers, enterprise systems, and automated reporting tools, for instance, do not structure observability in identical ways, nor do they create the same scope for contextualisation, intervention, or challenge in practice (Kellogg, Valentine, & Christin, 2020; Leonardi, 2011).

At the same time, critical studies complicate organisational accounts of surveillance by emphasising how digital systems can intensify asymmetries of knowledge, control, and extraction, while labour process theory situates surveillance within broader struggles over managerial control, consent, and discipline (Braverman, 1998; Edwards, 1982; Eubanks, 2018; Zuboff, 2019). Feminist and post-colonial perspectives further suggest that surveillance is not neutral in its effects, but is embedded in wider relations of power and control; thus, raising questions about what resistance challenges, what it accommodates, and whether moderating surveillance is always desirable (Gill, 2019). Studies on counter-surveillance and sousveillance similarly foreground tactical reversals of visibility and watching back as ways of contesting surveillance (Mann, Nolan, & Wellman, 2003; Taylor & Dobbins, 2021).

Nonetheless, research continues to treat surveillance as a managerial control tool, embedded within sociotechnical infrastructures (Ball, 2021; Kayas, 2023; Kayas, McLean, Hines, & Gillian, 2008). This framing constructs managers as the architects and executors of surveillance, responsible for selecting, deploying, and operating systems that collect data to evaluate employees. As a result, managers are often depicted as a homogeneous group, unquestioning in their adoption of surveillance because they are motivated by organisational interests. Here, we observe two shortcomings. First, surveillance studies focus overwhelmingly on its implications for employees, examining how monitoring is often interpreted through privacy, autonomy, trust, stress, fairness, uncertainty, and broader judgments about whether oversight is proportionate or legitimate (Ball, 2021; Kayas, 2023; Ravid, Tomczak, White, & Behrend, 2020). While such research provides an important starting point, showing how surveillance is experienced by those most commonly targeted by its effects, it also offers a point of contrast, as managers occupy a more complex position as actors who can simultaneously implement, interpret, and contest surveillance. Second, extant research fails to recognise the diversity of managerial roles, ranging from team leaders to senior executives, and that surveillance systems constrain and shape managerial agency. Consequently, managers are rarely theorised as actors subject to or affected by surveillance (Ball & Margulis, 2011; Kayas et al., 2025).

2.2. Managerial resistance to surveillance

Surveillance systems are not merely imposed but actively negotiated, contested, and resisted through sociotechnical processes (Ball, 2002). Resistance thus reflects an attitude or action that opposes the use of surveillance systems (Valtonen & Holopainen, 2025), enabling actors to

disrupt or subvert data flows when gaps appear in the technology-mediated relationship between observer and observed (Ball, 2010). This is especially salient in digital settings, where algorithms, analytics, dashboards, automated reporting, and other data-intensive systems extend how work is rendered visible, interpreted, and governed (Alshallaqi, 2024; Kayas et al., 2025; Kellogg et al., 2020; Valtonen & Holopainen, 2025).

Research has argued that resistance to digital systems can arise because of individual factors such as lack of awareness, lack of understanding, unwillingness to learn, status quo bias, and individual differences, alongside organisational issues like flawed implementation, talent shortages, or perceived imposition, and technological barriers including poor usability, malfunctions, system inflexibility, and overuse (Krishnan & Krishnan, 2025; Tseng, Yen, Hung, & Wang, 2008; Valtonen & Holopainen, 2025). However, while research shows how digitally mediated surveillance and algorithmic management systems generate resistance and compliance through mechanisms such as decontextualisation, trust, privacy concerns, fairness perceptions, and organisational practice, managers remain under-theorised as agents of resistance (van Zoonen, von Bonsdorff, & van der Heijden, 2025).

Indeed, most studies position employees as the primary agents of resistance, exploring obstructive responses to surveillance (e.g., Ball, 2005, 2010; Clawson & Clawson, 2017). These studies highlight that surveillance is not deterministic but shaped by an organisation's particular sociotechnical dimensions (Ball, 2002; Kayas et al., 2025). Ball (2005), for instance, situates resistance at the intersection of technology and human actors, based on two assumptions: (1) subordinates are autonomous agents who interact with technologies and superordinate observers, and (2) resistance emerges when surveillance is recognised and rejected as abnormal and unnatural. While this work provides important insight into how resistance is enacted, it continues to privilege the manager–employee dynamic, with analytical attention centred on employee responses (Martin, van Brakel, & Bernhard, 2009). From this perspective, employee responses to surveillance may include resistance in the form of masking, selective compliance, reinterpretation, and other tactical adjustments that interrupt surveillance without amounting to outright refusal, as well as tactical accommodation, neutralisation, and voluntary co-operation, complicating any simple opposition between surveillance and agency (Marx, 2003; Park, 2021).

Turning our focus from employee resistance to managerial resistance is crucial because the latter does not always emerge due to low awareness, usability barriers, or status quo bias, but can arise from ethical commitments, political accountability, and professional discretion (Bowman & West, 2021). Questions about whether, why, or how managers resist the surveillance systems they must implement and use (even when subject to them) are seldom raised. Research subsequently fails to account for how surveillance is enforced and contested at different organisational levels, especially in local government authorities, where heightened demands for accountability, transparency, efficiency, and public service ethics have led to the increasing deployment of surveillance (Charbonneau & Doberstein, 2020; Kayas et al., 2019; Natan-Krup & Mizrahi, 2025).

This omission is notable in public sector organisations because managers are not homogeneous, and accountability pressures, public service demands, bureaucratic discretion, and organisational visibility vary across administrative settings, shaping how surveillance is justified, enacted, interpreted, and resisted (Natan-Krup & Mizrahi, 2025; Pérez-Durán, 2024). The local government context is important not simply because it is public sector, but because it combines political accountability, service proximity, and managerial discretion in ways that make contextual judgement especially salient (Natan-Krup & Mizrahi, 2025; Pérez-Durán, 2024). It also leaves underexplored how managerial resistance may vary by hierarchical position, discretionary authority, and accountability relations, even though managers may simultaneously co-operate with, mediate, and resist surveillance in practice (Charbonneau & Doberstein, 2020; Kayas et al., 2019). This is important because more radical accounts of technological emancipation emphasise unmaking or refusing controlling systems altogether (Sabie, Soden, Jackson, & Parikh, 2023), whereas managerial resistance in local government settings may be more partial, reformist, and internally situated.

Further, the principles and standards underpinning public service ethics guide conduct in public administration, emphasising fairness, integrity, care, and respect for those served, while shaping how managers interpret and respond to surveillance as they balance organisational accountability with their ethical duties to employees and citizens (Bowman & West, 2021; Demmkea et al., 2025). These ethical principles are not operationalised solely through formal codes, but through the interaction of rules, leadership, management, and organisational environments in everyday practice, all of which shape how managers judge whether surveillance is legitimate, proportionate, or in need of contestation (Downe, Cowell, & Morgan, 2016; Perlman, Reddick, & Demir, 2023). Managers therefore confront competing ethical commitments in responding to surveillance, as accountability, transparency, fairness, care, and professional discretion may pull in different directions and create dilemmas over whether to comply with, reinterpret, or resist monitoring practices (Ehrich, Cranston, & Kimber, 2004; Lawton, 2005). Ethical commitments are thus better understood as cultivated through ethical competency, ethics management, and the wider ethical environment, which in turn shape how managers justify and enact resistance, rather than treated as fixed individual traits (Menzel, 2015).

3. Methodology

This study aims to examine how and why managers resist surveillance systems within the context of a local government authority. We collected data through semi-structured interviews, observations, and documentation and used a grounded theory approach to explore the social and technological processes through which managerial resistance emerges and is understood. This approach enabled theoretical insights to be generated directly from participants' lived experiences and organisational realities (Glaser & Strauss, 1967). Grounded theory is well suited to exploring how meaning and action develop within complex, hierarchical local government authorities, because it attends to the interplay between structure, agency, and context, capturing how managerial behaviour is shaped by the sociotechnical and ethical conditions of public service work. Following Strauss and Corbin (1990), open, axial, and selective coding were employed to identify, categorise, and connect patterns within the data. Through iterative analysis, and while using prior research insights as our sensitising devices, theory emerged inductively while remaining sensitive to the contextual realities of local government authorities. This provided analytical flexibility and theoretical depth, ensuring that the resulting interpretation reflected how managers construct, contest, and justify resistance. Finally, findings were cross-examined with existing literature to refine and situate the theoretical interpretation within wider debates on surveillance and resistance.

3.1. Research context

The research was conducted within a UK local government authority that was purposively selected as a theoretically relevant case for examining managerial resistance to digitally mediated workplace surveillance. The council was well suited to this study because systems for performance reporting, workforce monitoring, and managerial oversight were already embedded in routine organisational practices. It also enabled comparison across managers in different hierarchical roles and departments, allowing the study to examine how resistance varied under different organisational conditions within the same context. This provided a contextually grounded basis for theoretical development by capturing variation in managerial responsibilities, experiences of surveillance, and resistance practices within the same organisational

environment. The case was therefore particularly useful for examining resistance in a local government authority where digital oversight was already embedded across multiple functions. Further, approaching this through the perspective of a single case study allowed us to consider multiple sources of evidence, and to understand managerial resistance across hierarchies and within a real-life setting (Yin, 2009). Notably, the study focused on surveillance as embedded in routine organisational practice, rather than during a discrete crisis, restructuring episode, or other critical event. To ensure confidentiality, the local government authority and all participants were anonymised, and pseudonyms were assigned.

Council Alpha employs over 10,000 people, providing public services to a population of approximately 220,000 residents. It is governed by elected councillors representing local wards and operates under a leader and cabinet executive model. This governance structure has formal lines of political and managerial accountability that shape how performance information is produced, reviewed, and acted upon. Council Alpha's core systems include an enterprise system, performance reporting tools, and the Microsoft Power Platform, which enable cross-departmental analytics and managerial oversight through performance indicators. Regular workforce analytics reports are produced on dashboards to track employee performance. Council Alpha has adopted other digital tools to modernise internal workflows, including management reporting and human resource processes. Together, these systems indicate a relatively developed digital infrastructure for oversight and reporting. The culture within Council Alpha also placed strong emphasis on accountability, reporting, and performance visibility, while still leaving space for managerial discretion and contextual interpretation in everyday practice. This culture and these technologies have increased the visibility of employee activities, extended managerial oversight, and contributed to the growing datafication of public services.

3.2. Data collection

Data were collected through 26 interviews with managers at different hierarchical levels and across multiple departments (Table 1). We engaged in theoretical sampling (Urquhart, 2022) to ensure variation in managerial roles, responsibilities, and exposure to surveillance technologies, providing multiple perspectives on how these systems were experienced and contested. Participants had to have relevant knowledge or experience of the digital systems used to manage, monitor, or evaluate work. Interviews were conducted in person or online, depending on participant preference. A semi-structured format was employed, guided by core themes, allowing flexibility to pursue emergent issues and participant specific experiences. This approach encouraged participants to reflect on their interpretations, actions, and ethical considerations in relation to surveillance. Interviews lasted 43–87 min and were audio recorded with consent.

Observations were conducted during staff meetings, training sessions, performance reviews, and informal managerial interactions to capture surveillance and resistance related practices and conversations. These were recorded in a field journal using shorthand notes to document organisational routines, managerial interactions, and interpretive discussions. The notes were organised around the setting, participants, and surveillance-related issues discussed, enabling attention to be paid to how monitoring practices, performance data, and managerial responses were articulated in situ. The observations provided complementary insight into how surveillance was discussed, rationalised, and resisted within everyday work. They also enabled comparison between managers' accounts and how surveillance-related issues were enacted, discussed, or negotiated in situated organisational settings. Documentary materials, including internal strategy papers, technical reports, and publicly available policy documents, were analysed to situate the empirical data within the council's institutional, political, and technological environment. Documents were selected for their relevance to performance monitoring, reporting systems, and managerial oversight, and were reviewed iteratively to identify how these practices were formally described and justified within Council Alpha. This helped to trace how surveillance was justified and framed within organisational discourse.

Table 1
Interviewee details.

Participant ID	Managerial Role	Department/ Function	Years in Council	Work Location
P1	Division Head	Social Care	5	Local Service Office
P2	Team Leader	Customer Services	2	Local Service Office
P3	Corporate Director	Communications & Marketing	5	Head Office
P4	Lead	Communications & Marketing	9	Local Service Office
P5	Team Leader	Social Care	15	Local Service Office
P6	Director	Transport & Environment	8	Head Office
P7	Division Head	Tourism	9	Local Service Office
P8	Team Leader	Communications & Marketing	2	Head Office
P9	Team Leader	Human Resources	22	Local Service Office
P10	Head of Services	Digital Systems	7	Local Service Office
P11	Lead	Social Care	1	Local Service Office
P12	Lead	Human Resources	11	Local Service Office
P13	Team Leader	Human Resources	7	Local Service Office
P14	Head of Services	Tourism	14	Head Office
P15	Team Leader	Communications & Marketing	4	Local Service Office
P16	Division Head	Estates	8	Local Service Office
P17	Division Head	Digital Systems	3	Local Service Office
P18	Head of Services	Highways	4	Local Service Office
P19	Director	Highways	13	Head Office
P20	Senior Executive	Finance	1	Head Office
P21	Senior Executive	Estates	14	Head Office
P22	Director	Finance	15	Head Office
P23	Team Leader	Highways	17	Local Service Office
P24	Director	Governance	7	Head Office
P25	Corporate Director	Highways	4	Head Office
P26	Team Leader	Finance	3	Head Office

The lead researcher's university ethics committee granted ethical approval. Formal authorisation to conduct the study was obtained from Council Alpha. All participants received detailed information about the research purpose and procedures, and provided informed consent before

taking part.

3.3. Data analysis

Interview data were transcribed using the built-in transcription function in Microsoft Teams. The transcripts were manually reviewed to correct transcription errors by listening back to the audio recordings and checking unclear passages against the original speech. Through this process, identifiable information was removed. Field notes taken during interviews were integrated into the transcripts to preserve contextual detail. Observation notes captured managerial interactions, meeting dynamics, and contextual factors surrounding surveillance, and were cross-referenced with interview data to enrich interpretation. Observation notes and documentary materials were analysed iteratively alongside the interview transcripts. These materials were read repeatedly to identify references to surveillance systems, reporting routines, managerial oversight, contestation, and attempts to contextualise or challenge system-generated information. The materials were then compared with the interview data during coding and memo writing to clarify organisational context, corroborate or complicate participants' accounts, and refine emerging categories concerning how managerial resistance was enacted, justified, and shaped within Council Alpha. Observation data were particularly useful for identifying how managers contextualised performance information in meetings, how surveillance was discussed in practice, and how resistance could remain subtle, routine, or only partially articulated in interviews.

Following screening and refinement, transcripts were manually analysed using open, axial, and selective coding (Table 2) (Strauss & Corbin, 1990). Coding was undertaken by the lead author, and interpretive rigour was supported through peer checking and discussion among the authors as categories and relationships were refined, with any differences in interpretation discussed until a shared understanding was reached. During open coding, transcripts were read multiple times to label discrete incidents, actions, and meanings related to managerial resistance. Axial coding was then used to explore relationships among categories, focusing on conditions, strategies, and consequences, with the emphasis being placed on developing a detailed description of the core categories. Through constant comparison, concepts were iteratively refined until categories achieved theoretical saturation. All interview transcripts were analysed in full during coding and constant comparison. Quotations included in the findings were selected as illustrative examples of patterns identified across the wider dataset, rather than as isolated pieces of evidence. Finally, during selective coding, emergent findings were compared with existing literature to strengthen interpretation and situate the contribution within debates on surveillance and managerial resistance. Here, we aimed to saturate our core categories, i.e., to identify all relationships between categories based on our data and the existing literature, with the view to accurately describe the phenomenon of managerial resistance. Table 3 outlines the stages of data analysis, showing how grounded theory was systematically and iteratively applied to explain managerial resistance to surveillance.

Table 2
Data structure.

Representative extracts	Concepts (open coding)	Subcategories (axial coding)	Categories (axial coding)
Self-protective motivation "Everything's traceable. One mistake, one bad day, and it's there forever" (P18). "Constant tracking makes me anxious about how things look up the chain" (P9). "I started keeping notes offline just to feel safe" (P25). "It's stressful knowing dashboards flag you for small delays" (P2). "I limit what I put in the system. Less data, less exposure" (P11).	Fear of unfair evaluation, job insecurity, desire to control visibility, avoidance of reputational damage, anxiety over data permanence	Perceived threat to autonomy, loss of trust, defensive data practices, stress avoidance	Resisting surveillance to safeguard job security, autonomy, and reputation
Value-driven motivation "I work in social care, not a call centre" (P5). "These targets take time from real casework" (P7). "I tell my team to close the system if it crashes. Fairness matters more" (P22). "We should treat staff with respect, not as data points" (P20).	Ethical objection to dehumanising metrics, protection of team well-being, commitment to fairness, upholding service values	Defence of professional integrity, moral justification for resistance, alignment with care and justice norms	Resisting surveillance to uphold fairness, proportionality, and public-service ethics
Shielding employees "I step in when metrics misrepresent staff performance" (P7). "I highlight off system work so no one's unfairly penalised" (P17). "I add comments before reports go to HR to explain context" (P18). "If your boss won't shield you, you're exposed" (P26). "You can't just let the system run	Protecting subordinates from punitive data, adding narrative context, using discretion to reinterpret reports, mediating between data and fairness	Managerial advocacy, contextual interpretation, ethical buffering, discretionary mediation	**Target:** Dashboards and performance culture **Enabler:** Comment fields and managerial authority **Nature:** Productive **Mode:** Individual, covert (tacit collective norm)

(continued on next page)

4. Findings

4.1. Managerial motivations for resistance

Managers described a variety of concerns motivating their decision to resist surveillance, often emphasising a need for self-protection while also revealing overlaps with personal preference and pragmatic self-interest. Many expressed unease about how performance metrics and surveillance are used to evaluate or discipline them unfairly, "*There's this constant feeling that your team's performance is being tracked. It creates a load of stress… You worry about how it'll be interpreted up the chain and what the consequences will be*" (P9). Other managers highlighted fears about reputational risk and exposure, "*Everything's traceable. One mistake, one bad day, and it's there forever. It makes you hesitant. Some of us*

Table 2 (*continued*)

Representative extracts	Concepts (open coding)	Subcategories (axial coding)	Categories (axial coding)
people over" (P12).			
Data obfuscation "I tell staff to log things however they need to" (P9). "I delay uploads, so others don't feel pressured." (P19). "I enter placeholder values to avoid unfair flags" (P15). "I use manual overrides if monitoring's too harsh" (P19). "We quietly adjust things where it makes sense" (P23).	Altering data timing, masking or minimising trails, exploiting system flexibilities, humanising rigid metrics	Pragmatic rule-bending, soft subversion, managerial discretion under pressure	**Target:** Dashboards and time-entry tools **Enabler:** System gaps and organisational tolerance **Nature:** Productive – risk of obstructive data distortion **Mode:** Individual, covert (culturally shared)
Discursive practices "I redirected discussion from performance failure to system faults" (P6). "I add notes explaining context like staff bereavement" (P15). "I argue 'regular' reporting doesn't always mean weekly" (P22). "I questioned whether indicators improve service or just bureaucracy" (P21). "I've said outright the system's not fit for purpose" (P12).	Reframing narratives, contextual explanation, using policy ambiguity, questioning legitimacy, assertive challenge	Narrative reframing, contextualisation, ambiguity exploitation, institutional challenge	**Target:** Performance discourse and policy language **Enabler:** Positional authority and interpretive flexibility **Nature:** Mainly productive; obstructive when confrontational **Mode:** Individual, collective; overt–covert spectrum

Table 3
Stages of data analysis.

Stage of coding	Key tasks	Outputs
Open coding	• Familiarising with interview transcripts, observation notes, and documentation through repeated readings and memo writing • Labelling discrete incidents, actions, and meanings as initial concepts • Comparing codes across participants to identify similarities and contrasts	Initial concepts that represent early meanings, actions, tensions, and interpretations relating to managerial motivations and resistance to surveillance
Axial coding (iterative)	• Grouping concepts into subcategories • Identifying relationships between subcategories and higher order categories • Developing linkages between conditions, actions, strategies, and consequences in relation to resistance – coding around the axis of the core categories.	Subcategories and categories that reflect emerging patterns and relationships in how managerial motivations and resistance forms, varies, and unfolds. Core categories: self-protective motivation, value-driven motivation, shielding employees, data obfuscation, discursive practices
Selective coding - Integration with literature	• Comparing emergent categories with existing theoretical insights • Refining category boundaries and clarifying variation in meaning • Strengthening theoretical interpretation by aligning grounded insights with established concepts in surveillance, resistance, sociotechnical systems, and public service ethics	Refined theoretical interpretation that integrates grounded empirical categories with sensitising concepts from the literature

are actively finding ways around it because you don't feel safe" (P18). For several managers, surveillance created a "*climate of hyper accountability*" (P5), pushing them to withdraw from systems or limit their digital footprint. For example, P25 was observed recording information on paper rather than entering updates directly into the enterprise system, explaining that this gave them control over digital records. While these accounts reflect a self-protective motivation rooted in concerns over job security, autonomy, and well-being, they also suggest that some resistance was driven by a desire to avoid scrutiny altogether, regardless of its legitimacy. Crucially, these concerns were expressed in relation to hierarchical visibility, with managers describing anxiety about how data would be interpreted by more senior leaders and what consequences might follow. In this sense, self-protective resistance was shaped not only by surveillance, but by unequal power over how surveillance data were interpreted and acted upon.

In contrast, others described their motivation to resist surveillance because of ethical commitments and a desire to uphold professional or organisational values. These managers framed surveillance as inconsistent with the ethos of trust and care associated with public service, "*I work in social care, not a call centre. Reducing me and my team to productivity stats goes against everything we stand for*" (P5). Another manager noted, "*These strict targets make it look like we're hitting numbers, but they just take time away from proper casework. Residents don't get better services just because a spreadsheet looks good*" (P7). Others felt responsible for protecting their teams from excessive scrutiny, "*Sometimes I tell my team to just close the system if it keeps lagging or crashing. I don't want them penalised unfairly because the performance reports make it look like they're not doing their job. We're here to support them, not police them*" (P22). Yet even these value-driven accounts were not immune to complexity. Some managers acknowledged that appeals to ethical considerations and professional values could serve as a convenient justification for avoiding inconvenient system requirements or protecting preferred working practices. These motivations were further shaped by managers' positional responsibilities, as participants described balancing accountability upwards with obligations of care and protection toward employees. As a result, managerial resistance emerged within, rather than outside, organisational power relations.

4.2. Managerial resistance activities

These self-protective and value-driven motivations shape three interrelated types of managerial resistance that reflect distinct strategies for responding to surveillance.

4.2.1. Shielding employees

A prominent form of managerial resistance involved managers

shielding employees from surveillance by intervening to protect their team from being negatively evaluated or penalised by metrics:

"*We've got these performance systems that flag people for being behind on tasks, and it just spits out these reports. But I know who's been off sick or covering for someone else. So, I just tell HR that we're on top of it, even if technically someone hasn't hit the target. It's my job to protect them from being penalised for circumstances that aren't their fault. It's interpreting things with context*" (P7).

Similarly, when observing a departmental performance review, P2 intervened when a report flagged an employee's low output. They explained that the figures excluded urgent casework completed off system, preventing the matter from being logged as underperformance. P17 also explained, "*The data doesn't show who stayed late or supported a colleague. I go out of my way to highlight that in meetings*." In other observed review discussions, managers similarly supplemented dashboard outputs with contextual explanations about workload, absences, or off-system tasks before performance concerns were escalated. These examples highlight how managerial resistance was enacted to contest reductive performance interpretations that threatened to misrepresent employee contributions, with managers positioning themselves as advocates who used their authority to mediate between system outputs and broader understandings of performance.

Shielding was especially associated with dashboards, flagged reports, and review discussions, where managers could still intervene interpretively by recontextualising visible metrics rather than altering the underlying data. The ability to do this was partly shaped by organisational position, with some managers better able than others to intervene credibly, negotiate upwards, and reshape how surveillance outputs were read. Shielding therefore depended not only on discretion, but on the power to ensure that contextual interpretations shaped organisational decision-making. However, some managers expressed uncertainty about how far shielding should go, "*There's a fine line between supporting someone and covering for performance issues. I do it because I think it's right, but sometimes I worry I'm letting things slide*" (P15). Here, the result was managerial stress and doubt, where shielding risked slipping into protection of underperformance, creating dilemmas about fairness and accountability. This indicates that while shielding was often justified through care and contextual fairness it could also conflict with transparency and accountability.

The targets of employee shielding were the people, performance culture, and system dashboards that relied on decontextualised metrics for decision making, "*It's the culture around the data that's the problem. People assume the system's numbers are gospel, and that's dangerous*" (P18). While observing a monthly performance meeting, P13 skipped over dashboard figures that would have highlighted one team member's recent drop in performance. P13 later explained to a division head that the employee had been covering additional duties for a sick colleague. These examples indicate that the resistance was directed at both technology and people, highlighting how resistance targets the social and technological dimensions underpinning surveillance. The outcome here was an immediate organisational effect: the employee was shielded from formal sanction, but the omission also created blind spots in performance reporting that senior leaders did not see.

Many managers were able to shield employees because they had access to systems with discretionary features or informal backchannels that allowed them to reinterpret or override outputs, "*The reporting tool lets me add comments before it goes to HR. I use that space to explain any discrepancies. That's often enough to stop it going further*" (P18). While observing a division head reviewing a report, they entered a detailed explanation in the system's comment field, reframing a flagged delay as a backlog caused by a system outage. This led senior executives to move to the next case without further scrutiny, which protected employees and ensured fairer treatment. It also shaped organisational decision-making by shifting senior executives' focus away from individual blame. These examples demonstrate how technical features, combined with managers' social knowledge and discretionary authority, created openings for resistance, where the ability to frame data contextually or insert narrative explanations functioned as socio-organisational affordances rather than mere technical loopholes. Reporting tools and comment fields were especially important here because they enabled managers to append context to visible outputs, making shielding more a matter of interpretive mediation than of direct data alteration. Such openings were not evenly available because authority, system access, and credibility varied across managerial positions. This suggests that the effectiveness of shielding depended on differential access to organisational resources and interpretive power, rather than on managerial goodwill alone. However, some acknowledged that this discretion was unevenly applied across teams, "*If your boss is willing to step in, great. But not everyone's that lucky. It depends on who's in your corner*" (P26). In this instance, the organisational outcome was inequity, as shielding varied by managerial style and access, leading to uneven levels of protection across the council.

Managers overwhelmingly described shielding employees as productive, viewing their actions as reinforcing values such as fairness, trust, and support, rather than undermining organisational goals, "*I wouldn't call it resistance in a negative sense. It's about maintaining morale and doing what's right. Otherwise, we'd lose people to burnout or disillusionment*" (P12). These employee outcomes (i.e., improved morale, reduced burnout, and enhanced trust) were consistently emphasised as central to why managers resisted. P5 reflected, "*You can't just let the system run people over. It's part of our role to intervene when needed. That's not obstructive, it's responsible management*." These narratives position resistance as an ethical response to the rigidity of surveillance. For managers, this affirmed their professional identity and ethical commitments, positioning resistance as a form of responsible leadership. For the council, managers framed their actions as contributing to a healthier work culture and protecting staff retention rather than as disrupting organisational objectives. However, where shielding created reporting blind spots or obscured ongoing performance issues, its consequences could become more obstructive for organisational accountability. Its ethical defensibility thus depended on whether contextual protection remained proportionate or began to conceal issues requiring organisational attention.

Employee shielding was typically undertaken individually, although it was often part of a broader unspoken practice across managerial layers, "*We don't talk about it formally, but most of us protect our teams from unreasonable scrutiny*." P7 confirmed, "*You learn over time how to manage upwards, sideways, and down*." While observing an informal exchange after a performance meeting, two managers discussed how they added context to flagged cases before reports went upwards, treating this as a routine part of protecting teams rather than an exceptional intervention. Although no explicit agreement was stated, the exchange suggested a shared understanding that misleading metrics should be moderated before attracting senior scrutiny. This shows how, at the organisational level, shielding shaped cultures of discretion even without explicit coordination. While there was no indication of formally organised collective resistance, these practices were socially embedded and informally shared, pointing to tacit collective norms that appeared to circulate through informal post-meeting exchanges and shared interpretations of system failures, misleading metrics, and unfair reporting consequences. Rather than being formally coordinated, these norms seemed to become embedded as managers repeatedly discussed similar problems with surveillance outputs and treated contextualisation as a routine part of responsible managerial practice.

Managers explained that their actions were not officially sanctioned and were carried out covertly to avoid drawing attention, "*You don't broadcast that you're pushing back. It's more about finessing the narrative*" (P1). Another noted, "*If someone upstairs found out I was softening my reports, I'd get called out for it. So, I keep it low key*" (P9). This suggests that while shielding is oriented toward ethical and professional goals, it must still navigate power dynamics that demand discretion. Indeed, the need for concealment reflected power asymmetries in which upward

challenge remained possible, but not always safe. The covert nature of shielding offered managers protection from sanction, but for the council the outcome was reduced transparency, as resistance reshaped reporting practices in ways that were not always visible or equitable.

4.2.2. Data obfuscation

Data obfuscation involves managers masking, distorting, or minimising data trails to limit how surveillance systems evaluate or penalise their teams or themselves. As one manager explained, "*If someone logs in and out at different times, I don't challenge it. We all know the system's unreliable, and sometimes I just tell them to log things however they need to. I'd rather have a happy team than a perfectly accurate timesheet*" (P9). During a system downtime, P2 was observed telling a team member to delay submitting their work until the following morning. They explained that late entries would avoid triggering a performance warning in the dashboard. For employees, these actions reduced stress and protected them from unfair penalisation, but for managers the outcome included anxiety about bending rules and fears that they were sending inconsistent signals. As P9 admitted, "*I do bend the data sometimes, but I worry it sets a precedent that makes it harder to hold others to account*" (P9). This highlights the tension between protecting their teams or themselves and maintaining organisational accountability. Ethically, this positioned managers between humane judgement and the obligation to preserve accurate reporting. It also suggests that, where overt challenge was less feasible, managers could rely on quieter forms of resistance that operated within the limits of their positional authority, especially where open contestation would have exposed them to greater challenge from above.

Data obfuscation primarily targeted specific technological features of surveillance systems, such as dashboards, automated performance trackers, and time-entry functions, along with the organisational reliance on these tools for monitoring compliance. By manipulating when and how data is entered or recorded, managers challenged the legitimacy of these sociotechnical arrangements. As a director noted, "*We've got targets, yes, but not everything can be reduced to numbers. I sometimes delay my uploads, so others don't feel pressured. The numbers don't tell the whole story*" (P19). When observing a routine reporting process, a manager postponed updating a performance field until additional contextual information could be clarified, indicating that the timing of data entry was sometimes managed strategically rather than treated as a neutral administrative task. Compared with shielding, data obfuscation was more closely tied to technologies that captured inputs directly, such as time-entry functions, performance fields, and automated trackers, because these offered greater scope for delay, omission, revision, or placeholder entries. For employees, this reduced the pressure of constant monitoring, while for the council it risked weakening the accuracy of performance data used for decision making.

Data obfuscation was enabled by gaps and flexibilities in the systems, "*The enterprise system allows manual overrides for time entries. It's supposed to be for errors, but I sometimes use it if I think the monitoring's been too harsh. It's there, so I use it*" (P19). In a weekly review session, P15 was observed bypassing a mandatory form submission by entering a placeholder value in a performance field, later saying that it was "*better than giving the wrong impression*" about a team member's pace. In another reporting task, a manager revised a flagged entry before submission, explaining that the original figure would have given an unfair impression of team performance. These statements reveal how organisational tolerance for technical shortcomings, combined with complex workflows, offer a space for masking data, justified through professional values or pragmatic judgments.

Enterprise systems, reporting fields, and time-entry tools were especially important here because they allowed managers to intervene in the production of data itself, rather than only in how completed outputs were discussed. At the same time, these opportunities depended on managers having sufficient control over reporting routines or workflow decisions to exploit system gaps in practice. Nonetheless, some managers acknowledged that exploiting these weaknesses unintentionally undermined the reliability of reporting systems, "*I try to be fair, but sometimes I wonder if I'm just adding noise to an already broken system*" (P16). This had mixed implications, with employees benefitting from more humane interpretations of their performance, but with managers sometimes worried that these practices contributed to misleading records, producing organisational-level risks of fragmented or unreliable reporting.

Managers often framed data obfuscation as a form of productive resistance. They used data obfuscation to humanise the system and correct what they perceived as unjust representations, "*We're not gaming the system to get out of work. We're trying to make sure people aren't penalised for things outside their control*" (P13). During a training session, P5 instructed their team to "*leave certain optional fields blank*" if they felt the data would be misleading, framing it as a way of preventing unnecessary scrutiny. While these actions involved subtle subversions, they aligned with broader organisational values around fairness, wellbeing, and context sensitive judgement. Thus, the outcome for employees was protection from unfair scrutiny, while for managers it was the ability to exercise discretion and preserve a sense of ethical responsibility. Yet, at the organisational level, the outcome was more problematic, with fragmented or distorted data flows that undermined consistency and long-term accountability. This suggests a more ambivalent form of resistance: productive for employees and managers in the short term, but potentially obstructive for organisational learning, data reliability, and accountability. Compared with shielding, its ethical justification appeared weaker where protecting staff depended on knowingly distorting data.

Although some examples hinted at a shared understanding across managerial levels, individual action was the dominant mode of data obfuscation, "*We don't really talk about it, but everyone knows you can't take the system too literally. We quietly adjust things where it makes sense*" (P23). With data obfuscation, this shared understanding was reinforced by repeated exposure to system limitations and by managers observing how peers quietly adjusted entries, delayed submissions, or used optional fields to avoid misleading performance signals. This suggests that although data obfuscation is rarely coordinated, it reflects a collective cultural orientation within certain departments that implicitly legitimises soft rule bending in the face of impersonal data logics. Its largely individual and quiet character also reflected the risks attached to more visible resistance within hierarchical accountability structures. This suggests that collective resistance remained muted not because shared concerns were absent, but because overt coordination carried greater reputational and organisational risk. For managers, this informality created discretion and autonomy, but at the organisational level it produced uneven application across teams, leading to inequities in how surveillance was resisted and data was reported.

Data obfuscation was largely covert, "*I'm not hiding something big, but I don't go telling everyone what I'm doing. I use my judgment to make sure the data don't misrepresent the work we're doing*" (P4). During a routine reporting task, a manager made small adjustments to entries without comment or discussion, and the activity passed as part of ordinary administrative work rather than as an explicit challenge to the system. This reinforces how resistance can be woven into everyday managerial discretion, functioning under the radar of formal accountability structures. Covert action offered managers protection from sanction, while for the council it reduced transparency, making it difficult to assess cumulative effects or reconcile practices with collective standards.

4.2.3. Discursive practices

Managers engaged in discursive resistance practices, using language to strategically challenge, reinterpret, or mitigate surveillance. When observing a performance review meeting, P6 redirected the discussion away from declining output figures, pointing instead to staff absences and unresolved IT faults. The shift reframed the conversation from performance failure to systemic issues, prompting a change in tone from

senior executives. In another review discussion, a manager similarly responded to a flagged performance issue by shifting attention to staff shortages and unresolved system delays, which redirected the conversation away from individual blame and toward broader operational constraints.

This overt and productive form of resistance allowed individual managers to reframe performance narratives while maintaining professional legitimacy. The target here is senior leadership's overreliance on performance metrics. For employees, the effect was protection from unfair judgments, while for managers it reinforced their professional role as contextual interpreters of performance. For the council, the implication was a temporary recalibration of attention, shifting the narrative away from individual blame toward systemic shortcomings. The enabler here is the director's access to multiple forms of contextual information unavailable to the analytics system, allowing them to credibly reframe data. Crucially, this depended not only on knowledge, but on having sufficient authority for that knowledge to carry organisational weight. Discursive practices were especially associated with review meetings, flagged reports, and other visible outputs that still required interpretation, because these settings allowed managers to challenge what the data appeared to mean without necessarily altering the data themselves. However, this ability to reframe performance narratives was not uniformly distributed across roles or teams, with hierarchical position shaping whose contextual knowledge carried weight and whose challenge could be overlooked. For example, during a meeting, P7 was observed attempting to contextualise a drop in performance figures, but the discussion moved on without engagement from senior managers, visibly frustrating P7. Here, the outcome was managerial disempowerment, as the attempt at reframing failed to influence organisational decision-making.

In an internal email chain, P15 was observed adding a detailed note explaining that a missed target was due to a member of their team dealing with a bereavement and an ongoing recruitment delay. While the numerical data remained unchanged, the message shifted the narrative toward empathy and operational constraints. Through strategic annotations and contextual notes, the manager subtly yet overtly reframed the data narrative, resisting a reductive, decontextualised interpretation of team performance. These practices reflect individual professional judgement and narrative control as key resistance tools. These individual and overt practices were framed as productive, aimed at humanising data and promoting fairness while remaining within acceptable professional boundaries. For employees, the effect was greater understanding and protection from punitive interpretations of performance metrics. For managers, the implication was a reinforcement of their professional identity as ethical leaders, though this also created dilemmas about being perceived as excuse-making. At the organisational level, the impact was more context-sensitive decision-making, but also the risk of diluting accountability when contextualisation blurred into selective representation. Yet, this use of discretionary narration also raised questions for some participants. While drafting a report, P23 debated whether to include contextual explanations for underperformance, expressing concern that doing so might be perceived as excuse making. Such examples highlight the potential tension between ethical framing and selective representation. It also indicates that even ostensibly productive discursive resistance could become more obstructive where contextualisation weakened consistent organisational scrutiny. Here, managers appeared to balance contextual fairness and professional discretion against consistency and accountability.

Several managers recounted how they individually used policy language to reassert their discretion, highlighting a covert and self-protective form of resistance aimed at delaying compliance with procedures without openly challenging them. This reinforced the enabling role of textual ambiguity, where policies written in broad or interpretive terms allowed managers to subtly redefine expectations without breaching compliance. Here, ambiguity functioned as a power resource, allowing managers to defend room for manoeuvre without directly confronting more senior authority. The discursive power lies in offering alternative readings rather than confronting rules directly. The target in such instances is the surveillance policy itself, "*When the policy says, 'regular reporting is expected,' I argue that 'regular' doesn't mean 'weekly.' It could mean monthly, depending on the service area. So, I'll say, 'We're meeting the requirement'*" (P22). Similarly, P25 reported, "*There's flexibility in how the policy's worded. I use that ambiguity to push back, saying things like 'Our interpretation is slightly different,' rather than flat out refusing to follow it*" (P25). For managers, this had the effect of reclaiming agency and protecting discretion in the face of rigid rules. For employees, it created greater flexibility in how work was reported, reducing pressure from blanket compliance. For the organisation, however, the impact was inconsistency in how policy was enacted, with ambiguity producing uneven standards across departments. This suggests that policy texts and reporting expectations invited discursive resistance differently from dashboards or enterprise systems, because they left more room for reinterpretation at the level of language and compliance meaning. This made discursive resistance ethically defensible when it clarified rigid rules, but more problematic when it produced uneven application.

Another manager described a more assertive form of discursive resistance, overt and occasionally obstructive, used as a form of advocacy to push for systemic improvements, "*I've flat out said in meetings that the system's not fit for purpose. I've said, 'If you want us to input this data, give us a system that doesn't crash every hour.' That gets their attention. It's not just venting. It forces a response*" (P12). In one meeting, a manager openly challenged the reliability of a reporting system and argued that continued data entry was unreasonable until recurring faults were addressed, prompting a more defensive response from senior colleagues and shifting the discussion toward the system itself. While still couched in professional language, the tone is sharper, signalling escalation rather than reinterpretation. This more assertive mode of resistance appeared more feasible where managers could draw on greater authority, legitimacy, or organisational standing. It also suggests that overt resistance was shaped by who had enough organisational power to absorb the reputational and political risks of speaking back. In this case, the effect for managers was influence coupled with reputational risk, for employees it offered the possibility of better designed systems, and for the organisation it created destabilisation of existing norms alongside potential for reform. This more confrontational example highlights the rhetorical spectrum of resistance from subtle reframing to direct institutional challenge, illustrating how discursive practices can simultaneously preserve, reshape, or destabilise surveillance norms.

5. A conceptual framework of managerial resistance to surveillance

Based on our findings, we developed a seven-dimensional conceptual framework for understanding managerial resistance to surveillance in local government, situated within existing literature on surveillance, resistance, sociotechnical systems, and public service ethics. Table 4 summarises the three types of managerial resistance. Resistance theory provides the foundation for classifying and interpreting why and how resistance occurs. The sociotechnical perspective explains how affordances and iterative adaptation loops enable, constrain, and transform resistance. Taken together, affordances and sociotechnical perspectives direct attention to how possibilities for resistance emerge through the interaction of system features, organisational routines, interpretive work, and managerial position, rather than from technology alone. This is important because surveillance and resistance are co-shaped in practice as managers work within, reinterpret, and sometimes redirect monitoring arrangements in everyday organisational life.

Further, public service ethics foregrounds the normative commitments managers hold, which shape motivations for resistance and its justification (Demmkea et al., 2025; Ehrich et al., 2004; Lawton, 2005;

Table 4
Summary of managerial resistance types.

Dimension	Shielding employees	Data obfuscation	Discursive practices
Self-protective motivations	May be present but not always foregrounded. Where shielding is linked to self-protection, it reflects anxiety about how performance data are interpreted up the hierarchy and concern about the consequences of visible underperformance for managers and their teams.	Strongly present. Data obfuscation aligns closely with self-protective concerns about unfair evaluation, reputational exposure, hyper-accountability, loss of autonomy, and the desire to limit scrutiny or retain control over digital records.	May be present, especially where managers use language strategically to manage exposure, preserve discretion, or reduce the organisational consequences of surveillance.
Value-driven motivations	Strongly present. Shielding employees is closely linked to care, contextual fairness, trust, and the duty to protect employees from excessive or unjust scrutiny.	Present, but ambivalent. Data obfuscation can be justified through humane judgement and fairness, especially where managers seek to prevent unfair penalisation, although these ethical justifications are more contested.	Strongly present. Discursive practices are closely linked to professional discretion, contextual interpretation, fairness, and the attempt to challenge reductive or misleading readings of monitored performance.
Target	People, performance culture, dashboards, flagged reports, and decontextualised performance interpretations.	Dashboards, automated trackers, time-entry systems, performance fields, enterprise systems, and compliance-oriented reporting routines.	Senior leadership interpretations, performance narratives, policy texts, reporting expectations, review discussions, and the meaning attached to system outputs.
Enablers	Interpretive authority, contextual knowledge, credibility with senior actors, access to comment fields or reporting tools, informal backchannels, and discretionary authority.	System gaps and flexibilities, manual overrides, reporting discretion, workflow complexity, technical shortcomings, and local control over data entry routines.	Access to contextual information, rhetorical skill, policy ambiguity, organisational standing, professional legitimacy, and authority to make alternative interpretations count.
Nature of resistance	Mostly productive, but with potentially obstructive effects. Often restores fairness and trust but can create blind spots or conceal ongoing issues.	Both productive and obstructive. Can protect employees and humanise the system, but also distort data, weaken accountability, and undermine organisational learning.	Mostly productive, but sometimes obstructive. Can humanise data and promote fairer judgement, but can also weaken consistency, dilute scrutiny, or create uneven policy application.
Mode of action: individual or collective	Predominantly individual, though often sustained by tacit collective norms and informal shared understandings across managerial layers.	Predominantly individual. Collective dimensions are weak and mostly implicit, rather than formally co-ordinated.	Predominantly individual, though some practices reflect broader shared norms about how to interpret and manage surveillance.
Mode of action: overt or covert	Often covert, especially when managers soften reports or shield teams without drawing attention. Can also be overt where context is inserted into visible reports or meetings.	Largely covert, operating through quiet adjustment, delay, omission, or revision within routine administrative work.	Varies from overt reframing in meetings and written reports to covert reinterpretation through policy ambiguity and subtle narrative work.
Managerial outcomes	Affirms professional identity and ethical leadership, but also creates stress, doubt, and risk where support is seen as excuse-making or concealment.	Preserves discretion and reduces immediate pressure, but creates anxiety about bending rules, setting precedents, and contributing to unreliable records.	Reinforces professional identity and agency where successful, but can also generate reputational risk, frustration, or disempowerment when reframing attempts are ignored.
Employee outcomes	Reduces unfair scrutiny, improves morale, protects trust, and lowers the risk of sanction or burnout.	Reduces pressure from constant monitoring and protects employees from unfair penalisation.	Improves contextual understanding of performance and protects employees from punitive or reductive interpretations.
Organisational outcomes	Can contribute to fairer treatment and retention, but also create blind spots, reduced transparency, and uneven protection across teams.	Can humanise rigid systems in the short term, but risks fragmented data, weaker accountability, reduced reliability, and inequity across departments.	Can support more context-sensitive decision-making and possible reform, but also create inconsistency, selective representation, or destabilisation of existing reporting norms.

Santoro & Cain, 2018), including how managers navigate tensions between care, fairness, transparency, accountability, and professional discretion. By integrating insights derived from the data with these theoretical perspectives, the framework conceptualises managerial resistance in local government as a socially embedded and technologically mediated organisational practice. Here, heightened political accountability, public service obligations, and professional ethics, shape motivations to resist, resistance types, and consequences (Downe et al., 2016; Perlman et al., 2023). The framework is thus grounded in a local government setting that combines political accountability, service proximity, and managerial discretion. These dynamics are also shaped by organisational hierarchy, as managerial position influences what forms of resistance are feasible, legitimate, and risky.

Motivations reflect the factors influencing a manager's decision to resist surveillance. Emerging from the grounded theory analysis, these motivations were refined through the literature. Contrary to employee-focused motivations that often stress adoption barrier explanations (e.g., Krishnan & Krishnan, 2025; Valtonen & Holopainen, 2025), for the purposes of developing a distinct account of managerial motivations, we adapt the distinction between instrumental and principled motivations

to resist (Santoro & Cain, 2018), by drawing from *self-protective* and *value-driven* motivations that coexist in local government contexts. Self-protective motivations, rooted in instrumental resistance, stem from risks such as reputational damage, threats to job security, and workload intensification, particularly where managers are exposed to upward scrutiny and heightened accountability for monitored performance. These pressures are amplified by technology features, such as automated alerts and real time monitoring, which reduce opportunities for discretion. Value-driven motivations, steeped in principled resistance, are rooted in public service ethics and the duty to uphold fairness, proportionality, and dignity, especially where managers understand their role as involving care and protection toward employees as well as accountability to senior actors. These motivations did not reflect a single ethical principle, but trade-offs between care, contextual fairness, professional discretion, transparency, and accountability (Ehrich et al., 2004; Lawton, 2005). Here, the sociotechnical configuration of metrics, workflows, and embedded norms may strip away context or misrepresent work processes (Ball, 2002; Ball & Margulis, 2011), prompting managers to resist surveillance systems on ethical grounds.

These underlying motivations influence the nature and content of the resistance activity. Depending on a manager's motivation, three types of resistance emerged. *Shielding employees* involves managers protecting staff from the negative consequences of surveillance through both technical and non-technical means. For example, buffering employees from counterproductive directives and shielding them from higher level pressure (Sutton, 2010). *Data obfuscation* reduces the clarity or completeness of information to limit its use for oversight, exploiting manual processes or ambiguous reporting fields (Brunton & Nissenbaum, 2011). *Discursive practices* operate in organisational discourse, using argument, persuasion, or reinterpretation to question or redefine the purpose of surveillance, drawing authority from both managerial status and domain expertise. These three activities also resonate with accounts of neutralisation, tactical accommodation, and partial co-operation, in which surveillance is modified, softened, or redirected without being rejected outright (Marx, 2003; Park, 2021). They also differ in the ethical values they most clearly express, with shielding aligning more closely with care and contextual fairness, data obfuscation with humane judgement under pressure, and discursive practices with professional discretion and contextual interpretation. These empirically derived types of resistance subsequently shaped the development of the framework's remaining dimensions. Indeed, the specific type of resistance managers enact in turn shapes its target, the enabling conditions it relies upon, its nature as productive or obstructive, and the mode of action through which it is enacted.

Target refers to what managers resist, which are typically integrated sociotechnical configurations. Technological targets can include dashboards, automated allocation systems, enterprise systems, reporting tools, analytics, and performance monitoring software, particularly when they impose narrow metrics or misrepresent complex work. These technologies do not structure observability in identical ways, but vary in the visibility, persistence, granularity, and contestability they create, which shapes the kinds of managerial responses they invite. Social targets include the organisational practices these systems enable, the actors who enforce them, and the institutional norms, cultures, and policies that legitimise their use.

Enablers are the social conditions and affordances that make resistance possible. Technological enablers include system features, including override functions, optional fields, or interoperability gaps that allow discretion in use (Choudrie & Zamani, 2016). Social enablers include professional solidarity, cross-departmental trust, organisational tolerance for discretionary decision making, and the positional authority needed to make resistance credible and actionable. In local government authorities, managers' statutory authority to interpret policy, combined with privileged access to system functions, can magnify these enablers (Kayas et al., 2019), although such access varies across hierarchical positions and shapes who can draw effectively on system discretion or negotiate upwards with senior actors. This highlights that affordances are relational action possibilities rather than fixed properties of systems. Indeed, the same override, comment field, or reporting gap could enable resistance for one manager but not another, depending on organisational standing, interpretive credibility, and wider sociotechnical conditions (Avgerou & McGrath, 2007; Leonardi, 2011).

Nature of resistance captures the distinction between productive and obstructive forms of resistance. Productive resistance involves managers using available affordances to alter surveillance systems in ways intended to preserve fairness, contextual judgement, professional ethics, or service quality (Courpasson et al., 2011). Such resistance is productive when it mitigates harmful or misleading surveillance effects without substantially weakening accountability, organisational learning, or reporting integrity. Obstructive resistance, by contrast, seeks to disrupt or reject surveillance without offering viable alternatives, exploiting one's hierarchical position, system knowledge, or technical flaws (Thomas, Sargent, & Hardy, 2011). However, this distinction is not fixed. The same activity may be productive for employees or managers, while becoming obstructive for organisational learning, data quality, or accountability. The nature of resistance is therefore best understood as context-dependent and dependent on whose interests are prioritised.

Mode of action refers to whether resistance is carried out individually or collectively and overtly or covertly. These dimensions intersect, producing varied expressions of resistance shaped by the organisational context, hierarchical position, and other sociotechnical conditions (Meier, Ben, & Schuppan, 2013). Managers with greater authority or organisational standing may be better able to resist overtly through discursive challenge or contextual reinterpretation, whereas others may rely more on less visible forms of resistance. In this sense, mode of action reflects not only organisational tolerance for dissent and affordances that either conceal or expose resistance, but also the fact that managers may simultaneously comply with, mediate, and resist surveillance within the same role.

Outcomes of managerial resistance may be described as the product of the sociotechnical resistance activity and reflect the combined social and technical effects for managers, employees, and organisations. As surfaced in the analysis, these outcomes are also shaped by organisational power relations and managerial position. For managers, resistance could restore agency, affirm professional identity, and uphold ethical commitments, but also create different levels of exposure to detection through system logging, oversight, or peer reporting. For employees, it may reduce punitive oversight, build trust, and preserve autonomy when surveillance controls are softened with legitimate managerial justification. For organisations, resistance can prompt system redesign, policy reform, and greater fairness, but may also create data blind spots or undermine performance metrics. The consequences therefore vary not only by resistance type, but also by whose resistance is recognised, tolerated, ignored, or challenged within the organisational hierarchy.

Together, these empirically grounded dimensions provide a synthesis of managerial resistance to surveillance a local government authority. Motivations influence the types of resistance, which target particular configurations and depend on enabling conditions. These, in turn, shape the nature and mode of action of resistance, while managerial positionality and organisational power relations influence which forms of resistance are feasible, credible, and consequential. Read from affordances and sociotechnical systems perspectives (Avgerou & McGrath, 2007; Leonardi, 2011), the framework shows that managerial resistance is woven into the enactment of surveillance itself, as managers reinterpret metrics, mobilise contextual knowledge, and selectively use or resist system features in practice. This demonstrates how surveillance and resistance are mutually shaped within everyday organisational routines, rather than appearing as separate phenomena with one simply reacting to the other. It also remains sensitive to the fact that these routines are shaped both by organisational setting and by the specific surveillance technologies through which visibility and intervention are enacted. The framework therefore shows how resistance is a dynamic

product of sociotechnical interplay, shaped by organisational, social, and political dynamics of public service as well as by the technical design of surveillance.

6. Discussion

6.1. Theoretical implications

This paper examined how and why managers resist surveillance systems within the context of a local government authority. It generated a theoretical account of managerial resistance grounded in the data and in dialogue with literature on surveillance, resistance, sociotechnical systems, and public service ethics.

Building on this foundation, the study extends the debate by challenging portrayals of managers as a homogeneous group of enforcers who implement and operate surveillance systems to evaluate employees and uphold organisational control (Ball, 2021; Ball & Margulis, 2011; Kayas, 2023). Instead, it shows that managers are not always compliant executors of surveillance, but may contest it in ways that are subtle, strategic, and contextually informed. Moreover, by conceptualising managers as a heterogeneous group with differences in responsibilities, authority, values, and ethical stances toward surveillance, the framework developed here extends earlier research that treats them as a uniform category serving organisational interests (e.g., Clawson & Clawson, 2017; Sewell & Barker, 2006). The analysis also shows that managerial resistance should not be understood as the simple opposite of co-operation with surveillance. Indeed, managers remain responsible for implementing, interpreting, and working within surveillance arrangements, which means that compliance, mediation, and resistance can co-exist within the same role and, at times, within the same practice. This is important because managerial resistance is enacted within organisational power relations, with managers contesting surveillance while still being bound by hierarchical duties, formal accountability, and unequal authority.

This study thus provides a more nuanced sociotechnical understanding of how resistance unfolds through hierarchical positions, social and organisational processes, and affordances, challenging the prevalent binary framing of "managers versus employees" (Ball & Margulis, 2011; Kayas, 2023; Kayas et al., 2008). Set against employee-centred studies, we elucidate how managers encounter surveillance from a dual position as both interpreters and targets of monitoring (Ball, 2021; Kayas, 2023; Ravid et al., 2020). This helps to explain why managerial resistance only partly aligns with prior research on public employees. Both groups may respond to surveillance through concerns about fairness, pressure, trust, and misrepresentation, but managers do so from an institutionally different position shaped by responsibility for implementation, upward accountability, and authority over others. Indeed, managers are embedded in hierarchical relations that require them to balance care downwards with accountability upwards, while having more uneven access to system features, contextual information, and interpretive authority through which resistance can be enacted.

Previous research acknowledges that employee motivations for resistance can arise from instrumental or principled concerns (Bowman & West, 2021; Santoro & Cain, 2018). Here, the analysis suggests that in this local government setting, managerial motivations are shaped by a similar duality, encompassing self-protective and value-driven logics that coexist and interact in context (Bowman & West, 2021; Charbonneau & Doberstein, 2020; Santoro & Cain, 2018). These motivations are embedded in the wider sociotechnical context of surveillance, aligning with research that highlights how affordances and social norms jointly influence the emergence and type of resistance (Ball, 2002; Ball & Margulis, 2011; Kayas et al., 2025). From a sociotechnical perspective (Avgerou & McGrath, 2007; Tangi et al., 2025), the analysis shows that managerial resistance is not merely motivated by a reaction to technological control, but a product of the interaction between social processes, system features, organisational norms, and professional ethics in local government contexts (Charbonneau & Doberstein, 2020; Downe et al., 2016; Kayas et al., 2019; Perlman et al., 2023).

At the same time, these motivations were shaped by positional responsibility, as managers described balancing accountability upwards to senior actors with obligations of care, protection, and fairness toward employees. The findings further suggest that self-protective motivations were tied to unequal power over the interpretation and use of surveillance data, whereas value-driven motivations were tied to managers' attempts to use their limited discretion to buffer employees from decontextualised forms of control. Importantly, value-driven resistance did not rest on a single ethical principle. Rather, managers appeared to navigate trade-offs between care, contextual fairness, professional discretion, transparency, and accountability (Ehrich et al., 2004; Lawton, 2005). This extends surveillance research focusing on employees by distinguishing how self-protective and value-driven motivations manifest among managers (Bowman & West, 2021; Warren, 2003).

These motivations gave rise to three distinct types of managerial resistance: (1) shielding employees, (2) data obfuscation, and (3) discursive practices. Each activity illustrates the situated ways in which managers in a local government authority contest surveillance, offering a granular understanding of resistance strategies as part of a multilayered and intentional response. The framework identifies the social and technological targets of these activities, including technological features of the surveillance systems, policies, and hierarchical expectations. It also unpacks the sociotechnical enablers, such as affordances, process ambiguities, and cultural norms, that create space for discretionary action (Avgerou & McGrath, 2007). Foregrounding these dimensions deepens sociotechnical accounts of resistance, showing that it emerges from the coupling of specific technological features (e.g., override functions, interoperability gaps) and social conditions (e.g., professional solidarity and discretionary authority).

The analysis further shows that affordances for these three types of resistance were relational and unevenly distributed. Override functions, reporting fields, workflow ambiguities, and access to contextual information did not carry the same possibilities for every manager. Instead, they became usable resources for resistance only where managers had sufficient authority, interpretive credibility, and organisational latitude to act through them. The findings also indicate that not all surveillance technologies invited the same forms of response. Dashboards, reporting fields, enterprise systems, and automated monitoring tools created different degrees of visibility, persistence, granularity, and contestability, which shaped the room managers had for buffering, reinterpretation, delay, or selective modification (Kayas et al., 2025; Kellogg et al., 2020; Leonardi, 2011). This means that managers were not simply responding to surveillance after the fact, but were actively involved in reworking how monitoring functioned in practice through buffering, reinterpretation, delay, and selective modification (Avgerou & McGrath, 2007; Kayas et al., 2025; Parker et al., 2025). Hence, managerial resistance is often tactical and partial, combining contestation with selective co-operation rather than outright refusal (Marx, 2003; Park, 2021). Indeed, the three resistance types were more often individual and covert than overtly collective, with shared concerns circulating informally across managerial layers but rarely becoming formally co-ordinated because of upward accountability, reputational risk, and fragmented authority. In contrast to more emancipatory accounts of technological unmaking (Sabie et al., 2023), the three types of resistance rework surveillance from within existing organisational arrangements.

The findings also advance the debate by indicating that the three resistance activities were not equally available across managerial roles. Indeed, aligned with previous claims (Ball, 2021; Ball & Margulis, 2011; Kayas, 2023; Kayas et al., 2025), the findings here suggest that managers with greater authority, legitimacy, or access to contextual knowledge were better positioned to reframe data overtly or negotiate upwards with senior leaders, whereas others relied more on quieter, covert, or

data-based tactics that operated within tighter constraints. Organisational power structures therefore shaped not only the feasibility of resistance, but also whether it was recognised, tolerated, ignored, or exposed. In this respect, power influenced more than the amount of resistance managers could enact. It shaped whose interpretations counted, whose discretion was protected, and whose contestation remained vulnerable to dismissal or sanction. Accordingly, whether resistance appears productive or obstructive depends partly on whose interests are prioritised and on the organisational consequences at issue. At the organisational level, these effects could accumulate over time. Where resistance was recognised, it could prompt reflection, redesign, and fairer oversight. Where it remained tacit or unevenly distributed, it could instead generate reporting blind spots, uneven protections across teams, and weaker accountability. Resistance could thus support fairness, contextual judgement, and staff well-being, yet still undermine system coherence and data reliability where tactics obscured systemic problems or created inconsistencies across teams (Warren, 2003).

These accumulated effects also have implications for organisational learning, understood here as the capacity of Council Alpha to adapt and improve its surveillance arrangements in response to problems identified in practice. Discursive practices were especially important because overt challenges to system reliability, misleading indicators, or policy ambiguity could function as informal learning signals, making visible where surveillance systems failed to reflect the complexity of public service work. However, such signals were more likely to support institutional learning where senior actors recognised them as legitimate feedback and connected them to governance routines, policy clarification, or system redesign. Where resistance remained covert, was dismissed as non-compliance, or took the form of data obfuscation that concealed rather than articulated system problems, it was less likely to support learning. Managerial resistance therefore has ambivalent learning consequences: it can expose the need for adaptation, but it can also fragment knowledge, hide recurring problems, and leave concerns dependent on informal discretion.

Read across hierarchical levels, the findings suggest a provisional pattern in how resistance was enacted. Managers, who were closer to day-to-day reporting routines, employee-level metrics, and operational performance pressures, tended to rely more heavily on shielding employees, contextualising dashboard outputs in routine reporting and review processes, and quieter forms of data obfuscation, including delayed entries or selective completion of reporting fields. By contrast, heads of service, division heads, directors, and senior executives were better positioned to deploy discursive practices overtly. For example, by reframing performance data in meetings, challenging system reliability, or negotiating interpretations of policy and reporting expectations in senior decision-making spaces. This pattern was not absolute, as higher-level managers could also shield employees, and lower-level managers could still engage in discursive challenge. However, hierarchy shaped which forms of resistance were safer, credible, and organisationally consequential, reinforcing the argument that managerial resistance depends not only on motivation or technology, but also on the positional authority from which managers act.

This also means that some resistance activities were more ethically defensible than others. Shielding and discursive practices were more readily justified where they restored context without materially distorting reporting, whereas data obfuscation raised sharper ethical concerns when protection depended on knowingly compromising data integrity. Critical surveillance scholarship further complicates this point by suggesting that resistance which appears productive in local organisational terms may still accommodate broader logics of monitoring and control by rendering surveillance more workable or legitimate (Eubanks, 2018; Zuboff, 2019). Productive resistance should therefore be interpreted as a situated and partial response, rather than as an unqualified challenge to surveillance itself.

Focusing on a local government authority generates new insights into how managerial resistance is shaped by bureaucratic structures, political accountability, and sector specific values (Bowman & West, 2021; Charbonneau & Doberstein, 2020; Downe et al., 2016; Perlman et al., 2023). This specificity matters because public sector organisations are not homogeneous, and local government combines political accountability, service proximity, and managerial discretion in ways that shape how surveillance is justified, enacted, and interpreted in practice (Charbonneau & Doberstein, 2020; Kayas et al., 2019; Natan-Krup & Mizrahi, 2025; Pérez-Durán, 2024). These institutional features also help explain why managerial resistance did not simply mirror the employee resistance literature. Indeed, in this setting, resistance was filtered through public accountability demands, managerial obligations to interpret policy and performance, and organisational expectations to mediate between system outputs and service realities. Whereas prior studies have centred on resistance in private firms and often treated managers solely as enforcers (e.g., Clawson & Clawson, 2017; Iedema, Rhodes, & Scheeres, 2006; Townsend, 2005), we show that local government managers resist not only to protect themselves and their teams, but also to uphold organisational ethics such as fairness, proportionality, and care. This expands the conceptual boundaries of research on resistance to surveillance by attending to sector specific dynamics, revealing that individualised, discretionary resistance, while often ethically framed, may remain siloed, uneven, and limited in impact unless recognised and addressed collectively (Charbonneau & Doberstein, 2020; Kayas et al., 2019; Warren, 2003).

6.2. *Practical implications*

For local government leaders and policymakers, managerial resistance is not inherently obstructive but can be a protective or ethical response to surveillance. Recognising this nuance is crucial for designing accountability systems that do not erode trust, discretion, employee well-being, or data integrity. Designing oversight systems without considering sector-specific constraints and public service values risks creating counterproductive workarounds. Overly rigid surveillance may lead managers to bypass or subvert technologies, undermining intended benefits. Local government authorities should therefore involve managers early in system design, build transparency and flexibility into implementation, and treat resistance as a signal of potential system misalignment rather than simply non-compliance. For policymakers, this suggests that digital oversight in local government should be governed not only as a technical instrument of accountability, but as a wider governance arrangement whose effects on discretion, fairness, data quality, and service quality require ongoing review. Policy frameworks should therefore support consultation, contextual review, auditability of discretionary overrides, and routes for ethical challenge where standardised metrics risk distorting complex public service work.

The findings also suggest that local government authorities should build structured mechanisms for contextualising surveillance data before it informs escalation, sanction, or formal judgments of employee performance. Shielding employees was often enacted through comment fields, narrative explanations, and managerial intervention in review discussions, indicating that managers need legitimate ways to explain absences, system failures, off-system work, workload pressures, and service complexity. Dashboards and performance reports should therefore include structured spaces for contextual explanation, and performance concerns should be reviewed through managerial judgement before being treated as evidence of individual underperformance. At the same time, the finding that managers sometimes engaged in data obfuscation suggests that local government authorities should audit patterns of manual overrides, delayed entries, placeholder values, and incomplete reporting. These practices should not be treated simply as compliance breaches. Instead, they should be treated as insight opportunities that can help improve the design of these system, because such practices can reveal where metrics, workflows, or reporting expectations misrepresent public service work. However, they also require governance attention because they can weaken data reliability, consistency,

and organisational accountability.

The findings further suggest that local government authorities should create safer and more systematic routes for managerial voice across hierarchical levels. Discursive practices show that managers can identify system faults, policy ambiguities, and misleading interpretations of performance data, but these concerns are not always heard equally because authority and credibility vary across roles. Regular forums that include team leaders, middle managers, directors, and senior executives could help surface concerns before they become covert resistance. Senior leaders should also be supported to distinguish between defensive avoidance, ethical challenge, and obstructive resistance, rather than treating all pushback as illegitimate. This matters because managerial resistance can function as an informal signal of where surveillance systems need redesign, policy clarification, or more proportionate use. Without such channels, resistance may remain tacit, unevenly distributed, and dependent on individual managerial discretion, leaving protection for employees uneven and difficult to govern across teams.

7. Conclusion

This paper offers a contextually grounded theoretical account of managerial resistance to workplace surveillance mediated by digital technologies within a local government authority. By shifting attention away from the dominant portrayal of managers as enforcers of surveillance, the study reveals the diverse motivations, types, and outcomes of managerial resistance for managers, employees, and organisations. It also shows that managerial resistance is shaped by positional responsibility, hierarchical relations, and organisational power, which influence what forms of resistance are feasible, credible, and risky. In doing so, it addresses longstanding gaps in surveillance research that overlooks managers as both subjects and mediators of surveillance (Ball & Margulis, 2011; Kayas et al., 2025) and responds to calls for more nuanced analyses of how sociotechnical configurations of digital systems shape organisational resistance (Avgerou & McGrath, 2007). The framework also extends existing theorisations by incorporating sector specific factors such as political accountability, public service ethics, and professional discretion (Bowman & West, 2021; Charbonneau & Doberstein, 2020; Demmkea et al., 2025).

While this paper provides important insights into managerial resistance to surveillance, it is based on a single UK local government authority. The framework should therefore be read as analytically grounded in this organisational setting rather than as a universally representative model across sectors or organisational forms. It is most readily applicable to larger and administratively complex local government authorities where digital oversight systems are already embedded in routine managerial practice. In smaller authorities, less digitally developed settings, or organisations with different surveillance infrastructures, the same resistance types may still occur but may take different forms and carry different constraints and consequences. In addition, the study examined surveillance under routine organisational conditions rather than during a critical event, and managerial resistance may take different forms during periods of restructuring, scandal, budgetary shock, or leadership transition. The data also did not contain clear instances in which managerial resistance was formally detected, sanctioned, or directly confronted by senior actors supportive of stronger surveillance. As a result, the study is better able to explain how managers enacted, justified, and interpreted resistance than how local government authorities respond when such resistance becomes visible or contested.

Future research could therefore examine managerial resistance across different sectors, national contexts, organisational sizes, and levels of digital oversight, as well as during critical events. Longitudinal work could also explore how resistance evolves over time, while future studies might extend the framework by examining additional resistance activities and variation across hierarchical levels, managerial roles, and organisational power relations. Relatedly, future research could examine cases where managerial resistance is detected, escalated, or challenged, including how senior actors supportive of surveillance respond, and whether such encounters lead to sanction, suppression, negotiation, or institutional learning. Future research could also examine more systematically how different surveillance technologies shape different forms of managerial resistance, particularly where technologies vary in visibility, granularity, contestability, and interpretive flexibility. In addition, comparative research across managers and employees could clarify where their resistance aligns, where it diverges, and how those differences are shaped by organisational position and responsibility.

Financial interests

The authors have no relevant financial interests to disclose.

Non-financial interests

The authors have no relevant non-financial interests to disclose.

CRediT authorship contribution statement

Oliver George Kayas: Methodology, Investigation, Formal analysis, Conceptualization, Writing – review & editing, Writing – original draft. **Efpraxia D. Zamani:** Methodology, Writing – review & editing, Writing – original draft.

Funding

The authors did not receive support from any organisation for the submitted work.

Declaration of competing interest

N/A.

Acknowledgements

None.

Data availability

The data are not available due to it containing information that could compromise the privacy of research participants.

References

Afzal, M., & Panagiotopoulos, P. (2024). Coping with digital transformation in frontline public services: A study of user adaptation in policing. *Government Information Quarterly, 41*(4), Article 101977. https://doi.org/10.1016/j.giq.2024.101977

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. *Government Information Quarterly, 39*(4). https://doi.org/10.1016/j.giq.2022.101721

Alshallaqi, M. (2024). The complexities of digitization and street-level discretion: A socio-materiality perspective. *Public Management Review, 26*(1). https://doi.org/10.1080/14719037.2022.2042726

Avgerou, C., & McGrath, K. (2007). Power, rationality, and the art of living through socio-technical change. *MIS Quarterly, 31*(2), 295–315.

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

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

Ball, K. (2005). Organization, surveillance and the body: Towards a politics of resistance. *Organization, 12*(1), 89–108. https://doi.org/10.1177/1350508405048578

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

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.

Bowman, J. S., & West, J. P. (2021). *Public service ethics* (3 ed.). Routledge. https://doi.org/10.4324/9781003203148

Braverman, H. (1998). *Labor and monopoly capital: The degradation of work in the twentieth century*. Monthly Review Press.

Brunton, F., & Nissenbaum, H. (2011). Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday, 16*(5). https://doi.org/10.5210/fm.v16i5.3493

Carter, C. (2025). AI surveillance: Reclaiming privacy through informational control. *European Labour Law Journal, 16*(2), 245–258. https://doi.org/10.1177/20319525241306327

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

Choudrie, J., & Zamani, E. D. (2016). Understanding individual user resistance and workarounds of Enterprise social networks: The case of service ltd. *Journal of Information Technology, 31*(2), 130–151. https://doi.org/10.1057/jit.2016.9

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

Courpasson, D., Dany, F., & Clegg, S. (2011). Resisters at work: Generating productive resistance in the workplace. *Organization Science, 23*(3), 597–906. https://doi.org/10.1287/orsc.1110.0657

Demmkea, C., Autioniemi, J., & Lenner, F. (2025). The end of the world as we know it – Public ethics in times of de-standardization and individualization. *Public Management Review, 27*(7), 1741–1763. https://doi.org/10.1080/14719037.2021.2000221

Downe, J., Cowell, R., & Morgan, K. (2016). What determines ethical behavior in public organizations: Is it rules or leadership? *Public Administration Review, 76*(6), 898–909. https://doi.org/10.1111/puar.12562

Edwards, R. (1982). Contested terrain: The transformation of the workplace in the twentieth century. *Science and Society, 46*(2), 237–240.

Ehrich, L. C., Cranston, N., & Kimber, M. (2004). Public sector managers and ethical dilemmas. *Journal of the Australian and New Zealand Academy of Management, 10*(1), 25–37. https://doi.org/10.5172/jmo.2004.10.1.25

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

Gill, R. (2019). Surveillance is a feminist issue. In T. Oren, & A. Press (Eds.), *The Routledge handbook of contemporary feminism*. Routledge.

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Aldine.

Iedema, R., Rhodes, C., & Scheeres, H. (2006). Surveillance, resistance, observance: Exploring the Teleo-affective volatility of workplace interaction. *Organization Studies, 27*(8), 1111–1130. https://doi.org/10.1177/0170840606064104

Ifenthaler, D., & Tracey, M. W. (2016). Exploring the relationship of ethics and privacy in learning analytics and design: Implications for the field of educational technology. *Educational Technology Research and Development, 64*(5), 877–880.

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly, 37*(3). https://doi.org/10.1016/j.giq.2020.101493

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., Chin, E. O., & Belal, H. M. (2025). From humans to algorithms: A sociotechnical framework of workplace surveillance. *Digital Business, 100120*. https://doi.org/10.1016/j.digbus.2025.100120

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., 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. *The Academy of Management Annals, 14*(1), 366–410. https://doi.org/10.5465/annals.2018.0174

Krishnan, M., & Krishnan, S. (2025). Investigating resistance to IT projects: A conceptual model from a meta-synthesis approach. *Information Technology and People, 38*(3), 1601–1629. https://doi.org/10.1108/ITP-10-2022-0809

Lawton, A. (2005). Public service ethics in a changing world. *Futures, 37*(2–3), 231–243. https://doi.org/10.1016/j.futures.2004.03.029

Leonardi, P. M. (2011). When flexible routines meet flexible technologies: Affordance, constraint, and the imbrication of human and material agencies. *MIS Quarterly, 35*(1), 147–167. https://doi.org/10.2307/23043493

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments [article]. *Surveillance and Society, 1*(3), 331–355. https://doi.org/10.24908/ss.v1i3.3344

Martin, A. K., van Brakel, R. E., & Bernhard, D. J. (2009). Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance and Society, 6*(3), 213–232. https://doi.org/10.24908/ss.v6i3.3282

Marx, G. T. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues, 59*(2), 369–390.

Meier, R., Ben, E. R., & Schuppan, T. (2013). ICT-enabled public sector organisational transformation: Factors constituting resistance to change. *Information Polity, 18*(4), 315–329. https://doi.org/10.3233/IP-130315

Menzel, D. C. (2015). Research on ethics and integrity in public administration: Moving forward. *Looking Back. Public Integrity, 17*(4), 343–370. https://doi.org/10.1080/10999922.2015.1060824

Misra, S., Katz, B., Roberts, P., Carney, M., & Valdivia, I. (2024). Toward a person-environment fit framework for artificial intelligence implementation in the public sector. *Government Information Quarterly, 41*(3), Article 101962. https://doi.org/10.1016/j.giq.2024.101962

Natan-Krup, D., & Mizrahi, S. (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

Park, Y. J. (2021). *The future of digital surveillance: Why digital monitoring will never lose its appeal in a world of algorithm-driven AI*. University of Michigan Press.

Parker, S. K., Ballard, T., Billinghurst, M., Collins, C., Dollard, M., Griffin, M. A., … Walsh, T. (2025). Quality work in the future: New directions via a co-evolving sociotechnical systems perspective. *Australian Journal of Management*. https://doi.org/10.1177/03128962251331813

Pérez-Durán, I. (2024). Twenty-five years of accountability research in public administration: Authorship, themes, methods, and future trends. *International Review of Administrative Sciences, 90*(3), 546–562. https://doi.org/10.1177/00208523231211751

Perlman, B. J., Reddick, C., & Demir, T. (2023). A compliance—Integrity framework for ethics management: An empirical analysis of local government practice. *Public Administration Review, 83*(4), 823–837. https://doi.org/10.1111/puar.13610

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.

Roztocki, N., Strzelczyk, W., & Weistroffer, H. R. (2025). Enterprise Systems in the Public Sector: Current research landscape. *Information Systems Management, 42*(2), 161–188. https://doi.org/10.1080/10580530.2024.2361617

Sabie, S., Soden, R., Jackson, S., & Parikh, T. (2023). Unmaking as Emancipation: Lessons and Reflections from Luddism. In *CHI '23: Proceedings of the 2023 CHI conference on human factors in computing Syste, Hamburg*. April 23–28.

Saldanha, D. M. F., Dias, C. N., & Guillaumon, S. (2022). Transparency and accountability in digital public services: Learning from the Brazilian cases. *Government Information Quarterly, 39*(2), Article 101680. https://doi.org/10.1016/j.giq.2022.101680

Santoro, D. A., & Cain, L. (2018). *Principled resistance: How teachers resolve ethical dilemmas*. Harvard Education Press.

Schubad, M., Bernards, B., van der Pas, S., & Groeneveld, S. (2026). Lost in translation how public managers across hierarchical levels shape customization depending on their managerial or professional identity. *Public Management Review*, 1–30. https://doi.org/10.1080/14719037.2025.2606829

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

Strauss, A. L., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Sage Publications Ltd.

Sutton, R. I. (2010). Managing yourself: The boss as human shield. *Harvard Business Review, 88*(9), 106–109.

Tangi, L., Müller, A. P. R., & Janssen, M. (2025). AI-augmented government transformation: Organisational transformation and the sociotechnical implications of artificial intelligence in public administrations. *Government Information Quarterly, 42*(3), Article 102055. https://doi.org/10.1016/j.giq.2025.102055

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

Thomas, R., Sargent, L. D., & Hardy, C. (2011). Managing organizational change: Negotiating meaning and power-resistance relations. *Organization Science, 22*(1), 1–285. https://doi.org/10.1287/orsc.1090.0520

Townsend, K. (2005). Electronic surveillance and cohesive teams: Room for resistance in an Australian call Centre? *New Technology, Work and Employment, 20*(1), 47–59. https://doi.org/10.1111/j.1468-005X.2005.00143.x

Tseng, P. T. Y., Yen, D. C., Hung, Y.-C., & Wang, N. C. F. (2008). To explore managerial issues and their implications on e-government deployment in the public sector: Lessons from Taiwan's Bureau of Foreign Trade. *Government Information Quarterly, 25*(4), 734–756. https://doi.org/10.1016/j.giq.2007.06.003

Urquhart, C. (2022). *Grounded theory for qualitative research: A practical guide*.

Valtonen, A., & Holopainen, M. (2025). Mitigating employee resistance and achieving well-being in digital transformation. *Information Technology and People, 38*(8), 42–72. https://doi.org/10.1108/ITP-05-2024-0701

Warren, D. E. (2003). Constructive and destructive deviance in organizations. *The Academy of Management Review, 28*(4). https://doi.org/10.5465/amr.2003.10899440, 662–632.

Yin, R. K. (2009). *Case study research: Design and methods* (4 ed.). Sage Publications Ltd.
van Zoonen, W., von Bonsdorff, M. E., & van der Heijden, B. I. J. M. (2025). Algorithmic surveillance and workers' compliance: The role of trust, privacy concerns, and fairness in online crowdwork. *Human Relations; Studies Towards the Integration of the Social Sciences*. https://doi.org/10.1177/00187267251379698
Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books Ltd.

Dr Oliver G. Kayas is a Senior Lecturer in Digital Business at Liverpool John Moores University Business School, UK. He has an established international research record and has published on the topics of workplace surveillance and information systems. His work has appeared in numerous top-ranked academic journals. As the President of the UK Academy for Information Systems, Dr Kayas leads the strategic advancement of teaching and research initiatives nationally and internationally. He is also a Director of the Board for the Surveillance Studies Network and an Associate Editor of the Surveillance & Society journal.

Dr Efpraxia D. Zamani is a Professor of Information Systems at Durham University Business School, UK. She received her doctorate from the Department of Management Science and Technology of the Athens University of Economics and Business (Greece). Her research interests are found at the intersection of organizational and social implications of Information Systems and emerging technologies. Her work has appeared in the Information Systems Journal, the Journal of Information Technology, Government Information Quarterly, and Technological Forecasting and Social Change, among others. In 2024 she received the AIS Sandra Slaughter Service Award.