E-ISSN: 3108-4192

APSSHS

Academic Publications of Social Sciences and Humanities Studies
2024, Volume 4, Issue 2, Page No: 74-82
Available online at: https://apsshs.com/

Journal of Applied Organizational Systems and Behavior

Digital Surveillance and the Breach of Psychological Contracts

Lina Hassan[1]*, Omar Khalaf[2], Reem Jaber[1], Rania Mostafa[3]

1. Department of Digital Surveillance and Psychological Contracts, Faculty of Business, University of Jordan, Amman, Jordan.
2. Department of Contract Breach and Trust, Faculty of Management, Jordan University of Science and Technology, Irbid, Jordan.
3. Department of Employee Relations, Faculty of Psychology, Al-Balqa Applied University, Salt, Jordan.

Abstract

Digital surveillance has become embedded in routine work through electronic performance monitoring, behavioral analytics, algorithmic evaluation, location tracking, communication analysis, and data-driven human-resource systems. Yet organizational scholarship often treats surveillance primarily as a technology, a control practice, or a privacy problem, leaving underdeveloped the question of when employees interpret monitoring as a failure of reciprocal organizational obligations. This Original Conceptual Framework Article proposes the Surveillance–Contract Interpretation and Repair Framework, an original non-empirical synthesis that positions surveillance as a potentially contract-relevant event rather than an automatic breach. The framework distinguishes surveillance architecture from enacted monitoring, formal permission from perceived legitimacy, privacy concern from attributed obligation failure, perceived breach from violation affect, and employee visibility from valid performance knowledge. It proposes that monitoring purpose, proportionality, contextual integrity, procedural fairness, trust, voice, and recourse may shape whether surveillance is interpreted as compatible with, ambiguous within, or contrary to the psychological contract. It further differentiates compliance, adaptation, gaming, voice, resistance, and withdrawal, and identifies acknowledgment, reparation, renegotiation, work redesign, and governance change as possible repair pathways. The framework generates testable propositions and specifies temporal, multilevel, measurement, and comparative research priorities. Its relationships remain conceptually plausible rather than causally validated. Applicability is conditional on employment arrangements, institutional protections, work design, prior trust, surveillance type, and organizational context. The contribution is an integrated vocabulary and research architecture for examining how digital surveillance becomes an employment-relationship event with consequences that cannot be inferred from technical capability alone.

Keywords: Surveillance as a psychological-contract event, Foundations of psychological contract theory, Privacy expectations and organizational obligations, Fairness, trust, and perceived breach, Research agenda, Methodological priorities

How to cite this article: Hassan L, Khalaf O, Jaber R, Mostafa R. Digital Surveillance and the Breach of Psychological Contracts. J Appl Organ Syst Behav. 2024;4(2):74-82. https://doi.org/10.51847/CmVpvAqfFN

Received: 30 November 2023; **Revised:** 25 January 2024; **Accepted:** 28 January 2024
Corresponding author: Lina Hassan
E-mail ✉ lina.hassan@ju.edu.jo

Introduction

Digital surveillance is no longer confined to visible cameras or periodic managerial observation. Contemporary organizations can record communication patterns, screen activity, location, task completion, biometric indicators, customer ratings, and behavioral traces, then use these data to allocate work, evaluate conduct, or trigger intervention. These practices span electronic performance monitoring, algorithmic mechanisms of control, and digitally expanded behavioral visibility [1–3]. Their organizational significance therefore lies not only in what is collected, but also in who interprets the data, which decisions follow, and whether employees can understand, challenge, or correct the resulting inferences.

Prevailing accounts often isolate surveillance as a privacy intrusion, productivity instrument, compliance mechanism, or technical feature. Such framings are necessary but incomplete because the same tool can be enacted through different purposes, levels of discretion, and employment practices. Algorithms may effectively redesign tasks, schedules, feedback, and evaluative authority, thereby changing the job rather than merely observing it [4]. Monitoring effects also remain heterogeneous and conditional on design, transparency, invasiveness, and context [5]. A contract perspective adds a relational question: does the practice communicate that the organization has departed from obligations employees believed governed their treatment?

That question matters because perceived surveillance is associated with differences in worker well-being and job attitudes, although cross-sectional evidence cannot establish temporal or causal direction [6]. Less favorable responses could reflect monitoring itself, demanding jobs, insecurity, weak leadership, prior distrust, or wider organizational change. Conversely, surveillance introduced for safety, coordination, or employee support may be regarded as acceptable when its purpose, proportionality, and safeguards are credible. The analytical task is therefore not to presume harm, but to explain variation in interpretation while keeping technological capability separate from legitimate organizational authority.

Calling surveillance a psychological-contract event changes the unit of analysis. The focal issue is neither the device alone nor an abstract organizational policy, but an encounter in which capability, enactment, explanation, and prior expectations become connected. This event may be discrete, such as installation of tracking software, or cumulative, such as expanding data reuse across successive decisions. The event label is therefore proposed as an analytical device: it directs attention to interpretation and time without assuming that employees share one expectation or that an obligation was actually breached.

This article develops the proposed Surveillance–Contract Interpretation and Repair Framework. It is an original, non-empirical conceptual contribution that links surveillance architecture, enacted monitoring, attributed organizational obligations, fairness and trust appraisals, perceived breach, employee responses, and possible repair. The framework treats each connection as conditional and testable. It does not classify every privacy concern as breach, infer collective perceptions from individual reactions, or claim that surveillance produces uniform outcomes. Its purpose is to organize previously separated domains into a researchable process while preserving rival explanations, contextual boundaries, and the possibility that monitoring is interpreted as compatible with the employment relationship.

Foundations of psychological contract theory

Psychological contracts concern an individual's beliefs about reciprocal obligations between employee and organization. They are not identical to formal employment contracts, objective promise inventories, or general expectations about desirable treatment. A dynamic account emphasizes that psychological contracts can be maintained, disrupted, revised, and repaired as organizational events acquire meaning over time [7]. For surveillance research, this distinction is essential: a monitoring practice becomes contract-relevant only when an employee connects it to an obligation attributed to the organization, such as discretion, respectful treatment, proportional data use, or meaningful explanation.

Breach is likewise an interpretive judgment rather than a direct property of a technology. It concerns a perceived failure to fulfil an obligation; violation refers to an affective reaction that may follow but is conceptually distinct. Longitudinal evidence indicates that breach perceptions and citizenship or counterproductive behavior can influence one another over time [8]. Other process evidence suggests that breach may emerge from interconnected triggers rather than one isolated event [9]. Repeated changes in monitoring, unexplained secondary uses, inconsistent enforcement, or ignored objections may therefore matter cumulatively, but that surveillance-specific sequence remains proposed.

The contract lens also clarifies why downstream consequences should not be reduced to immediate dissatisfaction. Longitudinal evidence identifies effort–reward imbalance as one plausible pathway linking breach with later mental and physical health outcomes [10]. This does not mean that surveillance necessarily initiates such a pathway, nor that breach alone explains health variation. Work intensity, insecurity, managerial treatment, and pre-existing health can remain competing explanations. The evidence instead supports studying breach as a temporally consequential relational appraisal whose effects may unfold through established work-exchange mechanisms.

Alternative theories remain necessary. Job-demands perspectives may explain strain without invoking a contract, procedural-justice theories may explain unfavorable reactions without obligation attribution, and technostress may account for responses to system complexity or intrusion. The psychological-contract account earns explanatory value only when employees identify an organization-relevant obligation and judge that its fulfilment has changed. Team discussion may amplify or stabilize such interpretations, but shared exposure cannot be assumed to produce a team-level contract. These distinctions make the framework complementary to, rather than a replacement for, established accounts of control, justice, exchange, and work design.

The proposed framework accordingly separates five concepts: exposure to surveillance, interpretation of organizational obligations, perceived breach, violation affect, and behavioral response. These stages may overlap empirically, but they should not be measured as substitutes. It also treats the employee as the primary locus of psychological-contract interpretation while recognizing that shared practices, team climates, and institutional arrangements may shape those interpretations.

Organizational-level claims require evidence of aggregation or collective processes; widespread use of one monitoring system does not by itself demonstrate a shared psychological contract or uniform breach.

Privacy expectations and organizational obligations

Workplace privacy is not simply the absence of observation. It concerns contested expectations about access, purpose, control, and appropriate information flow. Employees may accept one monitoring practice yet reject another depending on what is collected, who receives it, why it is used, and whether it affects consequential decisions. Privacy scholarship, contextual evaluations of monitoring, and analyses of personal integrity jointly show that surveillance disputes involve competing expectations, situational judgments, and employees' capacity to remain more than decontextualized data objects [11–13]. These concerns are related, but none alone establishes psychological-contract breach.

Organizational obligations may arise from explicit policies, managerial assurances, established practices, professional norms, or patterns of treatment from which employees infer reciprocal commitments. The proposed framework adds purpose limitation, proportionality, data accuracy, retention, secondary use, explanation, correction, and recourse as candidate obligation domains. A human-rights-based privacy due-diligence approach provides one model for prospectively identifying and mitigating employee-data risks [14]. Its legal force varies by jurisdiction, so it is used here as a governance rationale rather than a universal statement of law.

The key proposed mechanism is obligation attribution. An employee may dislike surveillance without believing that the organization promised otherwise; another may infer breach when formally permitted monitoring contradicts a credible assurance of autonomy or confidential use. Formal permission therefore differs from substantive legitimacy, and policy disclosure differs from genuine consent under employment dependency. Voice opportunity also differs from consequential influence: an organization may solicit views while retaining unchanged purposes, data flows, and decision authority.

Obligation attribution also requires attention to organizational referents and levels. Employees may attribute a disputed practice to a direct manager, a human-resource function, a platform, senior leadership, or an impersonal system, and these referents may not be interchangeable. A manager who cannot alter a centralized monitoring rule may still shape explanation and interpersonal treatment, while an organization may retain responsibility for data architecture that local managers merely enact. The proposed framework therefore locates perceived obligations at the individual level but treats formal policy, governance structures, and managerial enactment as distinct contextual sources of interpretation.

Table 1 organizes the evidence, constructs, relationships, uncertainties, and boundary conditions required for definitions, constructs, and conceptual boundaries for digital surveillance and the breach of psychological contracts.

Table 1. Definitions, constructs, and conceptual boundaries for Digital Surveillance and the Breach of Psychological Contracts.

Construct or component	Definition	Problem addressed	Distinction from adjacent concepts	Proposed role	Uncertainty	Boundary statement
Digital surveillance	Technology-enabled observation or inference about workers	Overly broad technology labels	Broader than one device or metric	Proposed event exposure	Practices change rapidly	Exposure is not breach
Behavioral visibility	Digital traces making actions or attributes observable	Assumed objectivity of data	Visibility is not valid performance knowledge	Proposed information condition	Interpretation may be inaccurate	Data do not speak for themselves
Psychological contract	Beliefs about reciprocal employment obligations	Confusion with written contracts	Subjective and relational	Proposed interpretive foundation	Content differs across employees	Belief is not legal entitlement
Privacy expectation	Belief about appropriate access, purpose, and use	Privacy reduced to secrecy	Distinct from complete non-observation	Proposed obligation content	Cultural and legal variation	Concern alone is not breach
Personal integrity	Capacity for contextual identity and agency	Employees reduced to data profiles	Broader than informational accuracy	Proposed appraisal domain	Direct effects remain untested	Normative risk is not measured harm
Fairness and legitimacy	Judgment that process and authority are justified	Favorable outcome treated as fairness	Legality and outcome favorability differ	Proposed appraisal pathway	Ordering with breach is uncertain	Unfairness is not identical to breach
Trust	Willingness to accept organizational vulnerability	Acceptance mistaken for confidence	Distinct from compliance	Proposed relational condition	Referent and timing vary	Compliance does not prove trust

Repair readiness	Capacity for acknowledgment, reparation, and redesign	Communication treated as sufficient repair	Distinct from restored trust	Proposed governance condition	Requires longitudinal validation	Readiness is not effectiveness

Note: Evidence-derived definitions are cited. Entries labelled proposed are original elements of the framework and are not validated relationships, thresholds, or universal prescriptions.

Fairness, trust, and perceived breach

Fairness and trust help explain why technically similar practices may produce different relational meanings. Fairness concerns the quality of procedures, information, interpersonal treatment, and outcomes; trust concerns willingness to accept vulnerability based on expectations about organizational competence, benevolence, or integrity. Experimental evidence indicates that reactions to algorithmic decisions vary with the nature of the managerial task rather than reflecting uniform algorithm aversion [15]. The framework therefore treats task type, decision stakes, and the balance between mechanical consistency and contextual judgment as moderators, not as fixed properties of surveillance. It also separates confidence in technical competence from trust in organizational intentions, because a system may be regarded as accurate while the purposes governing its use remain contested.

Procedural justice can remain weak even when an algorithm is introduced to reduce one form of bias, particularly when the process compresses people into limited attributes and omits relevant context [16]. Opacity adds a different problem: workers may react by inferring hidden rules, experimenting with behavior, and adapting to uncertain evaluative criteria [17]. Reductionism, opacity, and inaccuracy should not be collapsed. A system may be transparent yet reductive, accurate yet procedurally objectionable, or opaque without intentionally deceptive management. Each condition may shape breach interpretation through a different proposed pathway. Empirical work must consequently measure the appraisals separately rather than infer them from one global evaluation of the technology.

Algorithmic systems can also combine market coordination with organizational control. Evidence from platform work shows that matching, monitoring, compensation, and belonging tensions can arise together [18]. Such settings make power asymmetry particularly visible, but their employment arrangements limit direct transfer to conventional organizations. The proposed framework therefore distinguishes technological function from legitimate authority: the capacity to allocate tasks or predict behavior does not itself establish an accepted organizational right to do so, while formal managerial authority does not resolve whether its exercise is proportionate or contractually consistent.

Perceived breach is positioned after, but not mechanically determined by, these appraisals. An employee may judge surveillance unfair yet not infer a broken obligation; another may perceive breach because a trusted assurance about data use was contradicted even when the immediate outcome is favorable. Prior trust may buffer ambiguity, intensify disappointment, or shift the referent of blame. These alternatives require temporal testing, including the possibility that breach perceptions subsequently reduce trust or heighten sensitivity to later monitoring events. The framework consequently proposes fairness, legitimacy, and trust as separable, potentially interacting appraisals whose relation to breach is conditional rather than validated.

Employee resistance and withdrawal

Employee responses to surveillance should not be reduced to acceptance or overt opposition. Under algorithmic control, work can combine perceived autonomy, constrained agency, and anticipatory compliance rather than producing one uniform response [19–21]. Employees may value scheduling discretion while modifying conduct to satisfy ratings, rankings, or inferred rules. Compliance may therefore coexist with distrust, and apparent cooperation may conceal additional interpretive and emotional labor. Conversely, adaptation may be pragmatic rather than evidence of breach. The framework proposes that response classification must consider employees' attributed obligations, available alternatives, and dependence on the organization.

Resistance includes attempts to question, evade, reshape, or collectively contest monitoring. Organizational case evidence indicates that surveillance resistance is situated within institutional arrangements and workplace power relations [22]. Proposed responses range from selective invisibility, data withholding, metric gaming, and individual voice to collective challenge, reduced discretionary contribution, psychological withdrawal, or exit. These are not ordered stages or equivalent indicators of severity. A worker may game a metric to preserve task quality, remain silent because voice appears futile, or leave for reasons unrelated to surveillance.

The framework further proposes reciprocal dynamics. Unexplained adaptation may invite tighter monitoring; intensified monitoring may reinforce an employee's belief that discretion or good faith has been withdrawn. Managerial interpretation of resistance can also create escalation when legitimate contestation is reclassified as noncompliance. Yet workload, job insecurity, performance pressure, weak leadership, or technological frustration may explain the same behavior. Claims about withdrawal therefore require evidence linking surveillance exposure to obligation attribution and subsequent change over time.

Responses also differ in visibility and organizational meaning. Metric gaming leaves a trace that managers may detect, whereas psychological withdrawal may remain hidden behind continued task completion. Individual voice can become collective contestation only through interaction, shared interpretation, and sufficient relational or institutional support. The framework therefore rejects inference from isolated behavior to a common motive. Reduced communication, for example, may indicate distrust, workload, concentration, or adaptation to remote work. Research must connect observable responses to employees' stated interpretations without treating self-report as an infallible account of causation.

Table 2 organizes the evidence, constructs, relationships, uncertainties, and boundary conditions required for proposed mechanisms, relationships, and organizational consequences in digital surveillance and the breach of psychological contracts.

Table 2. Proposed mechanisms, relationships, and organizational consequences in Digital Surveillance and the Breach of Psychological Contracts.

Mechanism or relationship	Antecedent	Mediator or process	Moderator	Expected consequence	Rival explanation	Validation requirement
Autonomy–control tension	Flexible but datafied work	Proposed obligation appraisal	Worker dependence	Mixed acceptance and resistance	Self-selection into flexible work	Cross-context longitudinal tests
Visibility asymmetry	Unequal access to data and rules	Constrained agency	Experience and market position	Coping or selective resistance	Commercial competition	Compare occupations and power levels
Anticipatory compliance	Uncertain algorithmic criteria	Self-adjustment and extra labor	Perceived replaceability	Compliance with possible distrust	Community norm formation	Behavioral and within-person evidence
Situated resistance	Surveillance implementation	Interpretation and organizing	Institutional context	Contestation or modification	Wider change conflict	Comparative organizational cases
Breach–response feedback	Attributed obligation failure	Proposed reciprocal appraisal	Prior trust and voice	Escalation or recovery	Stable negative affect	Intensive longitudinal testing
Withdrawal pathway	Repeated adverse interpretation	Proposed disengagement process	Alternatives and insecurity	Reduced contribution or exit	Workload or career opportunity	Distinguish attitudes, intentions, and behavior

Note: Expected consequences and mediating processes marked proposed are original hypotheses. Evidence does not establish prevalence, causal order, effect magnitude, or universal transferability.

Possibilities for psychological-contract repair

Repair begins with distinguishing a disputed monitoring outcome from the relationship process that produced it. Experimental evidence indicates that breach-repair tactics are not interchangeable and that denial provides a weaker basis for repair than responses combining acknowledgment and substantive reparation [23]. In surveillance contexts, acknowledgment would require more than explaining that a system operated as designed. It may involve recognizing an unmet obligation, identifying inappropriate data use, correcting an inference, compensating a consequence, or accepting responsibility for inadequate safeguards. These practices are proposed applications; their durability in actual surveillance disputes remains untested.

Trust repair is temporal, relational, and potentially multilevel rather than a single communicative episode [24]. Employees may distinguish the trustworthiness of a manager, a human-resource function, senior leadership, and the technical system. Repair directed at the wrong referent may therefore fail even when it appears procedurally complete. Immediate acceptance of an apology also cannot establish restored trust. Credible assessment requires evidence of changed expectations and behavior over time, while allowing for spontaneous recovery, employee exit, or changing exposure as rival explanations.

Structural repair may require redesigning work rather than only improving messages. Digital technologies alter demands, autonomy, feedback, and decision authority through the work arrangements built around them [25]. Proposed repair may consequently include narrowing data collection, ending secondary uses, restoring human review, correcting historical records, creating usable appeals, and transferring decision responsibility back to accountable organizational actors. Employee participation should be consequential: consultation without capacity to alter purposes, rules, or remedies may reproduce the original concern.

Ethical governance must also address recursive organizational practices that normalize expanding data-driven control [26]. The framework proposes repair readiness as the organization's capacity to acknowledge disputed obligations, provide reparation, renegotiate expectations, redesign surveillance, and demonstrate consistency. Readiness is not an outcome, certification, or guarantee of restored trust. Some breaches may remain irreparable, and some monitoring may be non-negotiable for legitimate safety or legal reasons. The decision boundary is whether the organization can justify necessity and proportionality while preserving explanation, correction, and responsibility.

Proposed research agenda

The proposed SCIR Framework treats surveillance as a sociotechnical arrangement involving technology, organizational roles, knowledge, and power rather than an isolated algorithm [27]. Research should identify when architecture becomes

enacted practice, when practice activates obligation attribution, and whether privacy, fairness, legitimacy, or trust appraisals precede perceived breach. Competing direct pathways through workload, technostress, insecurity, or job design must be tested rather than absorbed into the framework.

Employment relations and institutional protections are central boundaries because worker dependence, contractual status, collective representation, and regulation shape both surveillance exposure and capacity to contest it [28]. **Figure 1** presents the original conceptual synthesis for research agenda, showing how the article's principal constructs, mechanisms, uncertainties, and decision boundaries are connected.

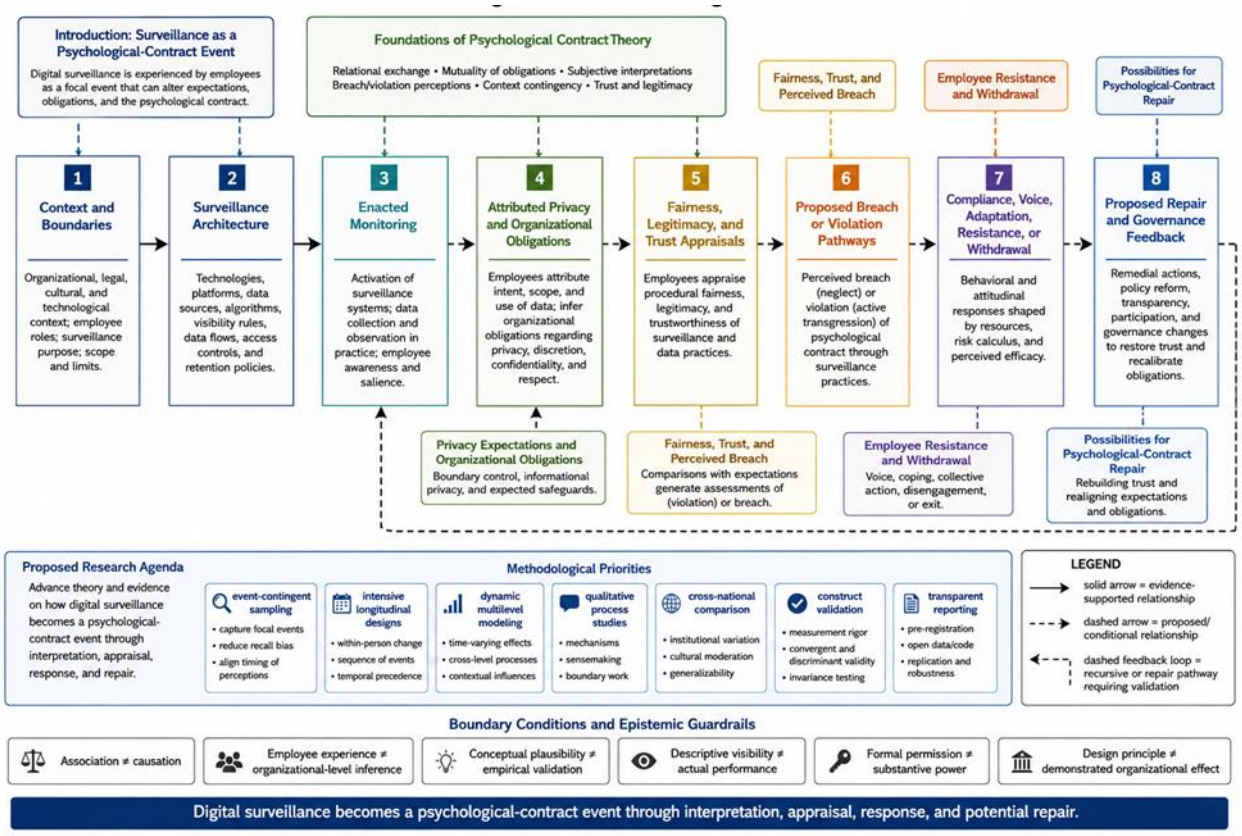

Figure 1. Research Agenda

Research should also test the dual possibility that algorithmic management constrains autonomy while creating value for workers, organizations, or customers [29]. **Table 3** organizes the evidence, constructs, relationships, uncertainties, and boundary conditions required for testable propositions, evaluation criteria, and practical responsibilities.

Table 3. Testable propositions, evaluation criteria, and practical responsibilities.

Proposition or criterion	Unit and context	Observable indicator	Evidence required	Falsification condition	Organizational responsibility	Misuse risk	Readiness boundary
P1 proposed: purpose drift increases obligation-failure interpretation	Employee within organization	Changed perceived data purpose and breach	Pre/post longitudinal evidence	No temporal association after confounds	Document and constrain uses	Treating disclosure as consent	Not ready without purpose tracing
P2 proposed: consequential voice weakens adverse appraisal pathways	Employee and team	Usable correction or appeal	Comparative field evidence	Voice quality predicts no difference	Provide influence and recourse	Symbolic participation	Not ready without outcome tracking
P3 proposed: autonomy loss and responsibility transfer interact	Job and work system	Discretion and accountable authority	Multilevel work-design evidence	Interaction fails across contexts	Align authority with responsibility	Blaming workers for system outputs	Not ready without role analysis
P4 proposed: repair requires reparation plus redesign	Relationship over time	Corrected practices and revised expectations	Longitudinal repair comparisons	Redesign adds no improvement	Acknowledge, remedy, and review	Performative apology	Not ready without sustained follow-up

Evaluation criterion: multidimensional ethics	Organization and stakeholders	Privacy, fairness, proportionality, inclusion, benefit	Triangulated governance evidence [30]	Criteria lack construct validity	Disclose trade-offs and affected groups	Ethics checklist substitution	Not ready as certification
Method criterion: rejectability	Multiple settings	Replication and rival-model comparison	Preregistered convergent designs	Simpler alternatives fit better	Permit independent scrutiny	Protecting the framework from refutation	Conceptual agenda only

Note: All propositions and readiness boundaries are original proposed elements. Indicators are research targets, not validated thresholds, legal determinations, or implementation standards.

The agenda should prioritize discriminating rather than merely confirmatory tests. Studies should compare the proposed contract pathway with justice, technostress, job-demands, and work-design models; examine whether obligation attribution adds explanatory value; and identify conditions under which monitoring remains relationally neutral or beneficial. Cross-level questions include whether managerial explanations offset centrally designed practices, whether team discussion produces shared breach climates, and whether collective representation changes recourse from symbolic access to consequential influence. Evidence against these propositions should refine or reject components rather than be treated as implementation failure.

Methodological priorities

Testing the framework requires temporal alignment between monitoring events and employee appraisals. Event-contingent or interval-contingent experience sampling can capture within-person changes while separating them from stable between-person differences [31]. Researchers should specify whether the focal event is exposure, discovery, explanation, decision use, objection, or repair. Sampling frequency must match the theorized process and minimize burden, reactivity, and selective nonresponse, particularly because heavily monitored employees may reasonably distrust additional data collection.

Dynamic multilevel models can estimate lagged and reciprocal relationships in intensive longitudinal data while separating within-person dynamics from between-person variation [32]. Such models could compare surveillance-to-appraisal, appraisal-to-breach, and breach-to-response paths, but lagged estimates do not establish causality. Designs should incorporate organizational changes, job demands, insecurity, prior trust, and exposure intensity as rival explanations. Team or organizational aggregation requires evidence of shared meaning and appropriate within-group agreement rather than common technology use alone.

Measurement is a primary validity boundary. Surveillance exposure, privacy concern, fairness, legitimacy, trust, breach, violation, voice, resistance, and withdrawal require explicit definitions and evidence that measures support their intended interpretations [33]. Researchers should test discriminant validity, measurement invariance, referent clarity, and sensitivity to change. Behavioral traces should not be treated as direct measures of psychological states, nor should self-reported breach be used as proof of an objective organizational failure.

Cumulative testing also requires transparent reporting of sampling, exclusions, construct decisions, missing-data handling, analytical alternatives, and deviations from planned analyses [34]. Strong programs should combine qualitative process studies, factorial experiments, longitudinal field designs, cross-national comparisons, and ethically governed trace–survey linkage. Convergence across designs would strengthen confidence; disagreement would identify boundaries or challenge the framework. Methodological sophistication cannot compensate for weak consent, intrusive measurement, or inability to protect employees from organizational access to research responses.

Because the subject is surveillance, research governance is itself substantively relevant. Participation should not expose workers to managerial retaliation, reveal identities through trace linkage, or imply that consent is freely given merely because employment continues. Data minimization, access separation, withdrawal procedures, and communication of study limits should therefore be documented as design features. Otherwise, a study intended to examine breached expectations may reproduce the asymmetry it seeks to explain.

Conclusion

Digital surveillance becomes organizationally consequential through more than observation. It may change work design, redistribute authority, expose behavior to new interpretation, and communicate how the organization understands its obligations to employees. The proposed Surveillance–Contract Interpretation and Repair Framework explains how those practices may become psychological-contract events through attributed privacy obligations, fairness and legitimacy judgments, trust, perceived breach, differentiated responses, and possible repair.

Its central boundary is equally important: surveillance is not breach by definition. Formal permission is not substantive legitimacy; visibility is not performance; consultation is not consequential influence; compliance is not trust; and apology is not demonstrated repair. The proposed sequence may vary, reverse, or fail to emerge across technologies, occupations,

employment relationships, institutions, and prior relational conditions. Alternative explanations through workload, insecurity, technostress, leadership, and work design remain necessary competitors.

The framework's contribution is therefore an integrated, rejectable research architecture rather than a validated causal model or organizational prescription. Progress depends on distinct measures, temporal evidence, multilevel discipline, comparison with rival models, and research practices that do not reproduce the surveillance problems under examination. Organizations may use the framework to ask more precise questions about purpose, proportionality, explanation, recourse, responsibility, and repair, but decision readiness requires context-specific evidence and sustained evaluation.

Acknowledgments: None

Conflict of interest: None

Financial support: None

Ethics statement: None

References

1. Ravid DM, Tomczak DL, White JC, Behrend TS. EPM 20/20: A review, framework, and research agenda for electronic performance monitoring. J Manag. 2020;46(1):100-26. doi:10.1177/0149206319869435
2. Kellogg KC, Valentine MA, Christin A. Algorithms at work: The new contested terrain of control. Acad Manag Ann. 2020;14(1):366-410. doi:10.5465/annals.2018.0174
3. Leonardi PM, Treem JW. Behavioral visibility: A new paradigm for organization studies in the age of digitization, digitalization, and datafication. Organ Stud. 2020;41(12):1601-25. doi:10.1177/0170840620970728
4. Parent-Rocheleau X, Parker SK. Algorithms as work designers: How algorithmic management influences the design of jobs. Hum Resour Manag Rev. 2022;32(3):100838. doi:10.1016/j.hrmr.2021.100838
5. König CJ. Electronic monitoring at work. Annu Rev Organ Psychol Organ Behav. 2025;12:321-42. doi:10.1146/annurev-orgpsych-110622-060758
6. Glavin P, Bierman A, Schieman S. Private eyes, they see your every move: Workplace surveillance and worker well-being. Soc Curr. 2024;11(4):327-45. doi:10.1177/23294965241228874
7. Rousseau DM, Hansen SD, Tomprou M. A dynamic phase model of psychological contract processes. J Organ Behav. 2018;39(9):1081-98. doi:10.1002/job.2284
8. Griep Y, Vantilborgh T. Reciprocal effects of psychological contract breach on counterproductive and organizational citizenship behaviors: The role of time. J Vocat Behav. 2018;104:141-53. doi:10.1016/j.jvb.2017.10.013
9. Wiechers HE, Coyle-Shapiro JAM, Lub XD, ten Have S. The tremors of interconnected triggers over time: How psychological contract breach can erupt. J Organ Behav. 2022;43(7):1172-89. doi:10.1002/job.2645
10. Griep Y, Bankins S, Vander Elst T, De Witte H. How psychological contract breach affects long-term mental and physical health: The longitudinal role of effort-reward imbalance. Appl Psychol Health Well Being. 2021;13(2):263-81. doi:10.1111/aphw.12246
11. Bhave DP, Teo LH, Dalal RS. Privacy at work: A review and a research agenda for a contested terrain. J Manag. 2020;46(1):127-64. doi:10.1177/0149206319878254
12. Vitak J, Zimmer M. Surveillance and the future of work: Exploring employees' attitudes toward monitoring in a post-COVID workplace. J Comput Mediat Commun. 2023;28(4):zmad007. doi:10.1093/jcmc/zmad007
13. Leicht-Deobald U, Busch T, Schank C, Weibel A, Schafheitle S, Wildhaber I, et al. The challenges of algorithm-based HR decision-making for personal integrity. J Bus Ethics. 2019;160(2):377-92. doi:10.1007/s10551-019-04204-w
14. Ebert I, Wildhaber I, Adams-Prassl J. Big data in the workplace: Privacy due diligence as a human rights-based approach to employee privacy protection. Big Data Soc. 2021;8(1):20539517211013051. doi:10.1177/20539517211013051
15. Lee MK. Understanding perception of algorithmic decisions: Fairness, trust, and emotion in response to algorithmic management. Big Data Soc. 2018;5(1):2053951718756684. doi:10.1177/2053951718756684
16. Newman DT, Fast NJ, Harmon DJ. When eliminating bias isn't fair: Algorithmic reductionism and procedural justice in human resource decisions. Organ Behav Hum Decis Process. 2020;160:149-67. doi:10.1016/j.obhdp.2020.03.008
17. Rahman HA. The invisible cage: Workers' reactivity to opaque algorithmic evaluations. Adm Sci Q. 2021;66(4):945-88. doi:10.1177/00018392211010118
18. Möhlmann M, Zalmanson L, Henfridsson O, Gregory RW. Algorithmic management of work on online labor platforms: When matching meets control. MIS Q. 2021;45(4):1999-2022. doi:10.25300/MISQ/2021/15333
19. Wood AJ, Graham M, Lehdonvirta V, Hjorth I. Good gig, bad gig: Autonomy and algorithmic control in the global gig economy. Work Employ Soc. 2019;33(1):56-75. doi:10.1177/0950017018785616

20. Curchod C, Patriotta G, Cohen L, Neysen N. Working for an algorithm: Power asymmetries and agency in online work settings. Adm Sci Q. 2020;65(3):644-76. doi:10.1177/0001839219867024
21. Bucher EL, Schou PK, Waldkirch M. Pacifying the algorithm—Anticipatory compliance in the face of algorithmic management in the gig economy. Organization. 2021;28(1):44-67. doi:10.1177/1350508420961531
22. Kayas OG, Hines T, McLean R, Wright GH. Resisting government rendered surveillance in a local authority. Public Manag Rev. 2019;21(8):1170-90. doi:10.1080/14719037.2018.1544661
23. Henderson KE, Welsh ET, O'Leary-Kelly AM. "Oops, I did it" or "It wasn't me": An examination of psychological contract breach repair tactics. J Bus Psychol. 2020;35(3):347-62. doi:10.1007/s10869-019-09624-z
24. Kähkönen T, Blomqvist K, Gillespie N, Vanhala M. Employee trust repair: A systematic review of 20 years of empirical research and future research directions. J Bus Res. 2021;130:98-109. doi:10.1016/j.jbusres.2021.03.019
25. Parker SK, Grote G. Automation, algorithms, and beyond: Why work design matters more than ever in a digital world. Appl Psychol. 2022;71(4):1171-204. doi:10.1111/apps.12241
26. Gal U, Jensen TB, Stein MK. Breaking the vicious cycle of algorithmic management: A virtue ethics approach to people analytics. Inf Organ. 2020;30(2):100301. doi:10.1016/j.infoandorg.2020.100301
27. Jarrahi MH, Newlands G, Lee MK, Wolf CT, Kinder E, Sutherland W. Algorithmic management in a work context. Big Data Soc. 2021;8(2):20539517211020332. doi:10.1177/20539517211020332
28. Duggan J, Sherman U, Carbery R, McDonnell A. Algorithmic management and app-work in the gig economy: A research agenda for employment relations and HRM. Hum Resour Manag J. 2020;30(1):114-32. doi:10.1111/1748-8583.12258
29. Meijerink J, Bondarouk T. The duality of algorithmic management: Toward a research agenda on HRM algorithms, autonomy and value creation. Hum Resour Manag Rev. 2023;33(1):100876. doi:10.1016/j.hrmr.2021.100876
30. Tursunbayeva A, Pagliari C, Di Lauro S, Antonelli G. The ethics of people analytics: Risks, opportunities and recommendations. Pers Rev. 2022;51(3):900-21. doi:10.1108/PR-12-2019-0680
31. Gabriel AS, Podsakoff NP, Beal DJ, Scott BA, Sonnentag S, Trougakos JP, et al. Experience sampling methods: A discussion of critical trends and considerations for scholarly advancement. Organ Res Methods. 2019;22(4):969-1006. doi:10.1177/1094428118802626
32. McNeish D, Hamaker EL. A primer on two-level dynamic structural equation models for intensive longitudinal data in Mplus. Psychol Methods. 2020;25(5):610-35. doi:10.1037/met0000250
33. Flake JK, Fried EI. Measurement schmeasurement: Questionable measurement practices and how to avoid them. Adv Methods Pract Psychol Sci. 2020;3(4):456-65. doi:10.1177/2515245920952393
34. Aguinis H, Ramani RS, Alabduljader N. What you see is what you get? Enhancing methodological transparency in management research. Acad Manag Ann. 2018;12(1):83-110. doi:10.5465/annals.2016.0011