Data Without Surveillance: Designing Trustworthy People Analytics Systems

Abstract

Organizations increasingly deploy people analytics and algorithmic management systems to improve productivity, equity, and decision quality. Yet the most common implementation pattern—passive, continuous, “invisible” monitoring—often undermines the very outcomes these systems are meant to improve by eroding trust, reducing motivation, degrading data integrity, and increasing resistance behaviors. Research syntheses and meta-analyses show that electronic monitoring is typically associated with greater stress and lower job satisfaction, with limited or no reliable performance upside; some evidence also links monitoring to counterproductive behavior and ethical drift. [1]

This whitepaper integrates three research streams—procedural justice, privacy calculus, and management research on surveillance and trust—into a practical design doctrine: **“Data Without Surveillance.”** In this doctrine, **trust is the gating factor** for people analytics adoption and for the validity of the data produced. Systems should therefore prioritize consent, transparency, explainability, and user control (including reversibility). We translate theory into product requirements for “RUDY AI,” including consent-based data collection, transparency dashboards, explainable metrics, trust measurement frameworks, adoption curves, KPI models, and A/B tests for transparency features. [2]

Executive Summary

Employee monitoring is often justified as necessary for productivity, compliance, or security. However, multiple research syntheses indicate that **monitoring’s net effect on key employee outcomes is generally negative**, and its performance benefits are frequently overstated. A large meta-analysis in an open-access journal found monitoring is associated with lower job satisfaction and higher stress, with essentially no relationship to performance and a small positive relationship to counterproductive work behavior. [3] A major review in *Annual Review of Organizational Psychology and Organizational Behavior* similarly concludes that the best current evidence points to neutral performance effects and small negative effects on attitudes and strain outcomes, with privacy invasion perceptions standing out as a substantial driver. [4]

Management scholarship has converged on a critical implementation insight: **monitoring is not psychologically neutral**. When it is experienced as surveillance, it signals distrust, increases perceived controllability by the employer, and triggers resistance and “metric gaming,” which in turn degrades data quality and organizational learning. [5] Harvard Business Review[6] articles aimed at practitioners highlight similar patterns: surveillance can erode trust and initiative and can backfire by encouraging rule-breaking rather than preventing it. [7]

This whitepaper's central premise is operational:

Trust is the gating factor for people analytics systems.
When trust is low, employees opt out, mask behavior, provide inaccurate self-reports, or disengage—producing biased data, unreliable models, and harmful managerial decisions. When trust is high, employees share higher-quality context, adopt tools voluntarily, and use insights for growth—producing a durable, compounding returns curve. This logic is directly supported by (a) procedural justice research emphasizing legitimacy and cooperation, (b) privacy calculus research emphasizing risk–benefit tradeoffs and trust, and (c) monitoring research emphasizing autonomy and perceived privacy invasion. [8]

We present a design approach that replaces surveillance with **consent-based, explainable, user-governed data flows**—and we tie it to measurable outcomes using an adoption curve model, trust measurement frameworks, and KPI instrumentation suited for product analytics and people analytics governance. [9]

Literature Review

Procedural justice as the backbone of legitimacy in data systems

Procedural justice research demonstrates that people's willingness to accept decisions and cooperate with authority depends heavily on whether the **process** is perceived as fair, respectful, and legitimate—often more than whether outcomes are favorable. [10] Tom R. Tyler[11] argues (across empirical synthesis) that legitimacy and perceived procedural fairness drive compliance and cooperation more effectively than deterrence-based approaches. [12]

For organizations designing people analytics systems, the procedural justice implication is straightforward: employees are not merely "data sources." They are subjects in a high-power-asymmetry context, where fairness judgments about how data is collected, interpreted, and used can determine whether employees cooperate, resist, or withdraw psychologically. [13]

A practical advantage of procedural justice as a design lens is measurability. The organizational justice literature provides validated, widely used measurement instruments that separate procedural, distributive, interpersonal, and informational justice—allowing organizations to detect *why* trust erodes (opaque procedures, disrespectful communication, unclear explanations, etc.). [14]

Privacy calculus, trust, and the limits of "rational consent"

Privacy calculus theory describes disclosure decisions as a tradeoff: individuals weigh perceived benefits against perceived risks and costs. [15] In practice, these judgments are strongly shaped by trust, context, and uncertainty—meaning "informed consent" is often fragile in real organizations, especially when employees fear retaliation or disadvantage if they refuse. [16]

Two bodies of evidence are especially relevant to workplace people analytics:

- **Procedural fairness can mitigate privacy concerns by increasing impersonal/institutional trust.** A well-cited study in *Organization Science* links information privacy concerns with procedural fairness and trust, suggesting that fair information practices can support willingness to disclose information in ongoing relationships. [17]
- **Individuals often struggle to navigate privacy tradeoffs**, because preferences are context-dependent and consequences uncertain. A major review in *Science* synthesizes behavioral evidence showing privacy decisions are shaped by uncertainty and context, undermining the assumption that employees can always calibrate "reasonable" disclosure on their own. [18]

For workforce sensing and wellbeing tracking specifically, researchers have questioned whether workers can meaningfully consent in contexts with structural power asymmetries; they argue consent must be *freely given, reversible, informed, and specific*—and that socio-technical supports are needed to approach that standard. [19]

Surveillance, monitoring, and the trust-performance paradox

The strongest empirical pattern in the monitoring literature is not "monitoring always harms performance," but rather:

1. Monitoring is widespread and expanding in scope (from output measurement into behavior, attention, location, and sometimes physiology). [20]
2. Monitoring tends to increase strain and reduce job satisfaction, with limited performance upside on average. [21]
3. Monitoring can backfire through social-psychological pathways: diminished autonomy, perceived distrust, and privacy invasion. [22]

A meta-analysis in *Computers in Human Behavior Reports* found monitoring slightly decreases job satisfaction and increases stress, shows no relationship with performance, and shows a small positive relationship with counterproductive work behavior—raising questions about monitoring as a productivity strategy. [3] The 2025 *Annual Review* article contextualizes these findings, emphasizing that privacy invasion and perceived intrusiveness are pivotal mechanisms and that evidence for performance benefits is inconsistent. [4]

A systematic review produced for the European Commission[23]'s Joint Research Centre similarly concludes that excessive monitoring is associated with negative psychosocial outcomes including increased resistance, decreased job satisfaction, increased stress, decreased organizational commitment, and increased turnover propensity—and stresses that surrounding policies and implementation choices materially affect the risk profile. [24]

Finally, the trust dimension shows up prominently in practitioner-oriented evidence. MIT Sloan Management Review[25]–published work on ethically monitoring remote workers emphasizes that surveillance can reduce productivity for employees who do not feel trusted and that organizations should reset boundaries and implement monitoring in ways that do not antagonize employees. [26] HBR similarly argues that surveillance can erode trust and place managers in a bind, and that monitoring can backfire by increasing rule-breaking. [27]

Theoretical Framework

A trust-gated model for people analytics

We propose a trust-gated socio-technical model: **design choices influence justice and privacy perceptions, which determine trust, which determines adoption, which determines data quality, which determines business value.** This is a causal chain supported by multiple literatures.

1. **Design features** (consent, transparency, explainability, control) shape perceived fairness and perceived respect. [28]
2. **Fairness and perceived privacy risk** determine trust in the system and in its operators (leadership, HR, managers). [29]
3. **Trust determines adoption behaviors** (opt-in, continued use, honesty of self-report, willingness to act on insights). McKinsey's work on AI adoption emphasizes that trust is foundational: if employees don't trust AI outputs and processes, they won't use them; explainability is a major mechanism that supports trust. [30]
4. **Adoption determines data integrity**. A monitoring-heavy system can collect "more" data, but if the behavioral signal is distorted by avoidance, productivity theater, and gaming, the system's inference quality—and downstream organizational decisions—degrade. Empirical work links monitoring to stress and job satisfaction reductions, and some work links monitoring to deviance via diminished agency. [31]

Why employees reject monitoring tools

From a research-grounded perspective, rejection is rarely because employees are "anti-data." It is typically because the system violates one or more of the following (measurable) conditions:

Autonomy and agency threat. Monitoring is frequently interpreted as control over *how* work is done, not just whether outcomes are achieved. Threats to autonomy are linked to worse motivation and wellbeing in organizational contexts, consistent with self-determination theory and workplace research. [32]

Privacy invasion and contextual mismatch. Privacy expectations depend on norms of "appropriate information flow" within a context; when workplace systems capture data that employees experience as outside those norms (e.g., home-life spillover, biometric inference), perceived violations intensify. [33] Helen Nissenbaum[34]'s contextual integrity framework is particularly useful in product design because it forces specification of *which* *data* flows, *between whom*, and *for what purpose*, and treats context violations as privacy harms. [35]

Procedural injustice. Covert deployment, ambiguous purposes, lack of voice, and lack of appeal pathways generate procedural injustice perceptions that predict lower cooperation and higher withdrawal. Classic research directly links monitoring methods, justice perceptions, and organizational citizenship behavior. [36]

Trust and power asymmetry. Even "consent" can be experienced as coerced in employment settings. Research on workplace wellbeing technologies argues that meaningful consent is structurally challenging and requires socio-technical safeguards, not just a checkbox. [19]

Behavioral and ethical backfire. Evidence suggests that monitoring can create conditions where employees focus on compliance theater rather than genuine ethical judgment and may increase rule-breaking or deviance under certain conditions. [37]

Trust as the gating factor

Trust is not a "soft" attitude; it is a system constraint that determines whether a people analytics platform has:

- **Coverage** (who participates),
- **Fidelity** (how truthful, representative, and context-rich the data is),
- **Control legitimacy** (whether insights are acted upon rather than resisted). [38]

A widely used trust model in organizational research defines trust as a willingness to accept vulnerability based on perceptions of the other party's ability, benevolence, and integrity. [39] Roger C. Mayer[40] and colleagues' framework is especially actionable for product design because each component maps to design-and-governance choices:

- **Ability:** model validity and reliability, clear error bounds, appropriate use domains.
- **Benevolence:** clear employee benefit, non-punitive defaults, support orientation.
- **Integrity:** adherence to declared rules (purpose limitation, access limitation), auditability. [41]

Complementarily, interpersonal trust research differentiates cognition-based trust from affect-based trust, allowing measurement of whether employees view governance as competent versus caring. [42] Daniel J. McAllister[43] provides validated constructs used widely in organizational settings. [44]

Productization: How RUDY AI Implements Data Without Surveillance

RUDY AI is specified here as a people analytics system designed to deliver measurable business outcomes without covert monitoring. The product design is grounded in three principles drawn from the research base: **procedural justice (legitimacy), privacy calculus (value exchange), and trust-by-design (adoption gating).** [45]

Consent-based data collection as the default

RUDY AI uses **affirmative, granular consent** rather than passive collection. This is consistent with scholarship showing that workplace consent is structurally difficult and must be supported by reversibility and specificity. [19] It also aligns with data protection principles emphasizing lawfulness, fairness, transparency, purpose limitation, and minimization. [46]

Operationally, consent is implemented as:

- **Purpose-bundled opt-ins** (e.g., "career development insights," "team collaboration diagnostics"), avoiding vague "analytics improvement" language that undermines privacy calculus clarity. [47]
- **Data minimization defaults**: the smallest data set that supports a declared use case is collected; expansion requires separate consent. [48] Ann Cavoukian[49]'s Privacy by Design principles reinforce "privacy as the default" and "privacy embedded into design," supporting this architecture choice. [50]
- **Reversible participation**: employees can pause data sharing, revoke consent for categories, and request deletion within feasible governance constraints—supporting meaningful consent rather than one-way extraction. [51]

Critically, "non-surveillance" is defined in product policy as: **no keystroke logging, random screenshots, webcam activation, biometric inference, or continuous location tracking for performance evaluation** unless a narrowly defined, legitimate safety or compliance purpose exists, with governance and worker representation. This follows the Joint Research Centre report's emphasis on psychosocial risks from expanding surveillance into broader aspects of personhood and home life. [24]

Transparency dashboards designed for procedural justice—not PR

RUDY AI includes employee-facing and governance-facing transparency dashboards that implement **informational justice** (the explanation component of organizational justice) and support trust calibration. [52]

Key elements:

- **Personal Data Ledger:** what data is collected, from where, for what purpose, retention window, and who can access derived outputs.
- **Use-Case Registry:** a list of analytics use cases with a "can/cannot" table (e.g., "cannot be used for disciplinary action," "cannot determine termination risk at the individual level"). Such purpose constraints are central to reducing perceived betrayal and moral violation risks described in people analytics downside research. [53]
- **Decision Traceability:** when a metric is surfaced to a manager or HR partner, the employee can see that disclosure occurred (what was shared and at what

aggregation level), enabling accountability. This is consistent with responsible AI guidance emphasizing governance and transparency to build stakeholder trust. [54]

- **Worker voice and appeal:** a built-in pathway for employees to contest interpretations ("this metric misrepresents my role")—a direct procedural justice mechanism. [55]

A design caution: transparency is not automatically beneficial in all contexts. Research on AI disclosure suggests that certain forms of disclosure can reduce trust, depending on context and evaluator beliefs—supporting the need to A/B test transparency mechanisms rather than rely on intuition. [56]

Explainable metrics that defend autonomy and reduce chilling effects

Explainability in RUDY AI is implemented at the level of *metrics* rather than "black-box scores," because procedural justice depends on whether a person can understand how they are being evaluated and whether the process seems policy-consistent and respectful. [57]

Metric design rules grounded in monitoring and algorithmic management research:

- **Outcome-linked over behavior-linked:** Prefer metrics derived from voluntary inputs, work outcomes, and employee-reported context rather than granular behavioral exhaust (which is more likely to feel invasive and distort work behaviors). [58]
- **De-emphasize "control metrics"** (time-on-task proxies). Evidence indicates monitoring is not reliably associated with performance improvements and can increase strain and counterproductive work behavior. [59]
- **Show input sensitivity:** Employees can simulate how changes in inputs affect outputs ("what would move this metric?"), supporting autonomy and reducing perceived arbitrariness. This aligns with research on the importance of understanding system outputs for trust and adoption. [60]
- **Confidence and uncertainty:** Provide uncertainty bounds and data sufficiency warnings, preventing overinterpretation and preserving integrity—the trustworthiness component in trust models. [61]

A research-backed governance layer: trust is partially institutional

RUDY AI treats trust as partly an institutional property, not only an interface property. Accordingly, it includes:

- **Policy enforcement:** purpose limitation, role-based access, retention limits, and audit logs aligned with core data protection principles. [62]
- **Worker representation:** the monitoring literature and EU synthesis emphasize that employee involvement in decision-making mitigates negative effects of monitoring implementations. [63]

- **Non-punitive defaults:** Monitoring guidance suggests developmental framing and learning-oriented use reduces harm relative to deterrence-oriented use. [64]

Hypotheses and Measurable Constructs

This section operationalizes the theory into testable hypotheses for a trust-first people analytics product.

Core hypotheses

H1: Procedural justice features increase trust and opt-in.
Employees exposed to justice-enabling features (voice, appeal, respectful and clear explanations, visible rules) will report higher procedural justice perceptions and higher trust in the system, leading to higher opt-in rates and sustained participation. [65]

H2: Consent granularity increases adoption and data quality.
Granular consent (category-level opt-in with reversibility) increases adoption and reduces defensive responding, improving the authenticity of self-report and reducing withdrawal behaviors. [66]

H3: Explainable metrics increase trust, but only when paired with clear employee benefit.
Explainability increases trust and usage when the value exchange is salient (privacy calculus benefits outweigh costs). Explainability without benefit framing may increase attention to risks and reduce trust for some users. [67]

H4: Surveillance-like data collection reduces trust and increases counterproductive and avoidance behavior over time.
Introducing monitoring-like features (even if technically "legal") reduces trust and increases stress and avoidance, degrading engagement and retention. [68]

H5: Transparency affects turnover intention through justice perceptions.
Greater transparency about algorithmic surveillance and evaluation improves justice perceptions and reduces intention to quit via procedural/distributive justice pathways, consistent with empirical findings in algorithmic management contexts. [69]

Measurable constructs and recommended instruments

Trust in system and institution * **Trustworthiness dimensions (ability, benevolence, integrity)**: adapt organizational trust items for "system + operator" as the trustee. [70] *Cognition-based vs affect-based trust**: separately measure confidence in competence vs relational care. [42]

Procedural justice and informational justice * Use organizational justice measurement that separates procedural and informational justice; these are directly sensitive to transparency, explanations, and voice mechanisms. [14]

Privacy concerns and perceived control * Use a multidimensional privacy concern instrument (collection, control, awareness) to quantify privacy calculus "cost" components and identify which aspect is driving opt-out. [71]

Perceived surveillance / privacy invasion * Treat perceived privacy invasion as a first-class construct given evidence that it is a strong driver of negative outcomes in monitoring contexts. [72]

Adoption and behavioral integrity * Opt-in, time-to-opt-out, feature engagement, and "honesty signals" (e.g., missingness patterns, extreme response patterns) should be tracked as behavioral indicators of trust gating. [73]

KPI Mapping and Adoption Curves

KPI model: opt-in, retention, engagement

A trust-first people analytics system must be measured like a product **and** like a governance program. The KPI model below is designed to quantify whether trust-building features translate into adoption and business outcomes.

Opt-in KPIs (coverage and legitimacy) * **Consent Opt-In Rate (COIR):** consenting employees / eligible employees, by data category (e.g., engagement pulse; development goals; collaboration metadata).
Consent Depth Index (CDI): weighted sum of opted-in categories, emphasizing higher-sensitivity categories (so "depth" is not confused with "volume").
Consent Reversal Rate (CRR): revocations / opt-ins. High CRR is an early warning signal of trust degradation or perceived purpose creep. [51]

Retention KPIs (durability and value exchange) * **30/90/180-Day Participation Retention:** continued participation in opted-in flows.
Opt-In Survival Curve: time-to-revocation distribution; segment by role, tenure, and manager.
Trust Recovery Rate: post-incident (policy change, press, internal rumor), the rate at which users re-opt-in after remediation. This treats trust as a dynamic stock, consistent with the monitoring literature's focus on implementation and context. [74]

Engagement KPIs (use and impact) * **Active Use Frequency:** number of sessions, dashboard views, or insight interactions per month.
*Action Conversion:** percentage of users who take at least one growth action (e.g., select a development goal, request coaching) after receiving insights. This ties people analytics to outcomes rather than surveillance. [75]

Adoption curves: modeling trust-first diffusion

People analytics adoption in organizations typically follows an S-curve: early adoption by innovators and early adopters, then scaling through a majority when social proof, workflows, and perceived legitimacy stabilize. [76] Two complementary models are useful:

- **Diffusion of Innovations** explains segment dynamics and the importance of social influence and perceived compatibility. [77]
- **Bass diffusion** provides an operational forecasting model separating innovation-driven adoption (p) from imitation-driven adoption (q), useful for rollout planning and benefits realization. [78]

RUDY AI can incorporate **trust as a parameter influencing both p and q**: * Trust raises p by reducing perceived personal risk for early adopters.
* Trust raises q by enabling positive word-of-mouth and reducing "infection" of skepticism following missteps. Monitoring research suggests missteps can quickly generate resistance and turnover propensity, which would show up as suppressed q or accelerated churn. [79]

KPI-to-business outcome linkage

To meet executive expectations (and avoid "ethics theater"), trust KPIs must be connected to business outcomes with explicit causal logic.

Higher trust → higher opt-in and retention → higher data coverage and integrity → better decisions → better engagement and retention outcomes.

The monitoring evidence base supports the risk side of this linkage: monitoring is associated with reduced job satisfaction and increased stress, and broader surveillance is linked to damaging mental health consequences. [80] If trust-first design reduces perceived surveillance and privacy invasion, it should shift these outcomes in favorable directions.

Experimental Design and Ethical Considerations

Experimental design: A/B tests for transparency and trust

Because transparency can help or harm depending on design, RUDY AI should treat transparency and explainability as **testable product hypotheses**, not moral assertions. [81]

A/B Test 1: "Personal Data Ledger" dashboard * **Control:** no dashboard; basic policy link only
*Treatment:** interactive ledger showing categories collected, purposes, retention, and access trails

Primary metrics: COIR, CDI, CRR, and 30/90-day participation retention.
Secondary metrics: procedural justice (procedural + informational justice scales), privacy concern (control/awareness), trust (integrity and benevolence subscales). [82]

A/B Test 2: "Why this metric?" explainability module * **Control:** metric presented as a score only
*Treatment:** explanation with inputs, uncertainty, and "how to improve" action path

Primary metrics: time on insight, action conversion, engagement frequency, and trust in system ability.
Moderators: baseline tech attitudes; baseline privacy concerns (IUIPC). Evidence shows AI disclosure and transparency effects may depend on evaluator attitudes, so segmentation is essential. [83]

A/B Test 3: Consent architecture * **Control:** single opt-in toggle
*Treatment:** granular consent by purpose + reversible controls + default-off sensitive categories

Primary metrics: COIR and CDI by category; CRR; opt-in survival curve.
Secondary metrics: perceived coercion / meaningful consent perception. Consent research indicates reversibility and specificity are central to meaningful consent in workplaces. [19]

A/B Test 4: Value exchange framing * **Control:** neutral request ("Share your data to improve insights")
*Treatment:** explicit benefit framing aligned to employee development ("Share X to receive Y," with guarantee of non-disciplinary use)

Primary metrics: opt-in and retention; action conversion.
Secondary metrics: perceived benefits vs perceived risks (privacy calculus). [84]

A/B Test 5: Manager-facing transparency + guardrails * **Control:** manager dashboards with broad visibility
*Treatment:** aggregation-first dashboards + embedded governance warnings + "do not use for" disclaimers and audit log visibility

Primary metrics: employee trust/justice perceptions within teams; turnover intention proxies; grievance signals.
Evidence in algorithmic management contexts suggests transparency is linked to justice perceptions and intention to quit via mediation pathways. [69]

Ethical considerations

A privacy-first, non-surveillance people analytics system must manage three ethical risks that standard product analytics often ignores:

Power asymmetry and "consent theater." Employment relationships constrain refusal. Research argues meaningful consent requires reversibility and structural protections, not only interface design. [19]

Function creep and integrity violations. Trust depends on integrity: if data collected for development is later used for discipline, layoffs, or covert performance ranking, trust collapses and future data becomes corrupted. This risk aligns with both organizational trust theory and privacy governance principles. [85]

Psychosocial harm and chilling effects. Evidence suggests surveillance can damage mental health and increase stress and disengagement. A non-surveillance design is not merely ethically preferable; it functions as risk mitigation to protect retention and productivity. [86]

Accordingly, RUDY AI's ethical commitments should be operationalized (auditable) as:

- **Purpose limitation & non-disciplinary use** by default (exceptions require explicit governance escalation). [62]
- **Aggregation-first analytics** and minimization of individual-level inference unless employee-visible and beneficial to the employee. [87]
- **Independent oversight** (e.g., cross-functional review council with worker representation), consistent with monitoring literature emphasizing participatory decision-making to mitigate harms. [88]
- **Privacy by design and default** as engineering principles rather than compliance afterthoughts. [89]

References

Ajunwa, I., Crawford, K., & Schultz, J. M. (2017). *Limitless Worker Surveillance*. *California Law Review*, 105, 735. [90]

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514. [18]

Ball, K. (2021). *Electronic Monitoring and Surveillance in the Workplace* (systematic review). Joint Research Centre, European Commission. [24]

Bujold, A., Parent-Rocheleau, X., & Gaudet, M.-C. (2022). Opacity behind the wheel: Transparency of algorithmic management, justice perception, and intention to quit. *Computers in Human Behavior Reports*, 8, 100245. [91]

Cavoukian, A. (2009/2011). *Privacy by Design: The 7 Foundational Principles* and related guidance. Information and Privacy Commissioner of Ontario. [92]

Chowdhary, S., Kawakami, A., Gray, M. L., Suh, J., Olteanu, A., & Saha, K. (2023). Can workers meaningfully consent to workplace wellbeing technologies? *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency*. [19]

Colquitt, J. A. (2001). On the dimensionality of organizational justice: Construct validation of a measure. *Journal of Applied Psychology*, 86(3), 386–400. [93]

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust. *Organization Science*, 10(1), 104–115. [94]

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. [95]

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. [96]

Glavin, P., Bierman, A., & Schieman, S. (2024). Workplace surveillance and worker well-being. *Social Currents*. [97]

Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. *Academy of Management Annals*. [98]

König, C. J. (2025). Electronic monitoring at work. *Annual Review of Organizational Psychology and Organizational Behavior*. [99]

Laker, B., Godley, W., Patel, C., & Cobb, D. (2020). How to monitor remote workers—ethically. *MIT Sloan Management Review* (accepted version). [26]

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355. [71]

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734. [39]

McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal*, 38(1), 24–59. [44]

McKinsey & Company. (2024). Building AI trust: The key role of explainability. [30]

McKinsey & Company. (2022). Why digital trust truly matters. [100]

Raveendhran, R., & Fast, N. J. (2021). Humans judge, algorithms nudge: The psychology of behavior tracking acceptance. *Organizational Behavior and Human Decision Processes*, 164, 11–26. [101]

Siegel, R., König, C. J., & Lazar, V. (2022). The impact of electronic monitoring on job satisfaction, stress, performance, and counterproductive work behavior: A meta-analysis. *Computers in Human Behavior Reports*, 8, 100227. [102]

Thiel, C. E., Bonner, J., Bush, J. T., Welsh, D. T., & Garud, N. (2023). Stripped of agency: The paradoxical effect of employee monitoring on deviance. *Journal of Management*, 49(2), 709–740. [103]

Tyler, T. R. (1990). *Why People Obey the Law*. Yale University Press. [104]

European Commission. (n.d.). Data protection explained: Principles of personal data processing under GDPR. [105]

Boston Consulting Group. (2025). A Promise That Brings AI to Life Responsibly (report, including HR "AI talent promise," dashboards, and feedback loops). [106]

---

[1] [3] [21] [31] [58] [59] [68] [80] [102] https://www.sciencedirect.com/science/article/pii/S2451958822000616

https://www.sciencedirect.com/science/article/pii/S2451958822000616

[2] [7] [27] https://hbr.org/2024/02/surveilling-employees-erodes-trust-and-puts-managers-in-a-bind

https://hbr.org/2024/02/surveilling-employees-erodes-trust-and-puts-managers-in-a-bind

[4] [49] [63] [72] [88] [99] https://www.annualreviews.org/content/journals/10.1146/annurev-orgpsych-110622-060758?crawler=true&mimetype=application%2Fpdf

https://www.annualreviews.org/content/journals/10.1146/annurev-orgpsych-110622-060758?crawler=true&mimetype=application%2Fpdf

[5] [20] [24] [38] [40] [74] [79] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC125716/jrc125716_electronic_monitoring_and_surveillance_in_the_workplace_final.pdf

https://publications.jrc.ec.europa.eu/repository/bitstream/JRC125716/jrc125716_electronic_monitoring_and_surveillance_in_the_workplace_final.pdf

[6] [98] https://journals.aom.org/doi/10.5465/annals.2018.0174

https://journals.aom.org/doi/10.5465/annals.2018.0174

[8] [10] [12] [28] [45] [55] [65] [104] https://www.des.ucdavis.edu/Faculty/Sabatier/Tyler1990.pdf

https://www.des.ucdavis.edu/Faculty/Sabatier/Tyler1990.pdf

[9] [78] https://pdodds.w3.uvm.edu/files/papers/others/1969/bass1969a.pdf

https://pdodds.w3.uvm.edu/files/papers/others/1969/bass1969a.pdf

[11] [26] https://centaur.reading.ac.uk/93709/1/Surveillance%20-%20and%20how%20to%20monitor%20remote%20working%20ethically%20%282%29.pdf

https://centaur.reading.ac.uk/93709/1/Surveillance%20-%20and%20how%20to%20monitor%20remote%20working%20ethically%20%282%29.pdf

[13] [19] [51] [66] https://dl.acm.org/doi/fullHtml/10.1145/3593013.3594023

https://dl.acm.org/doi/fullHtml/10.1145/3593013.3594023

[14] [52] [57] [82] [93] https://web.mit.edu/curhan/www/docs/Articles/15341_Readings/Justice/Colquitt_Dimensionality_of_Organizational_Justice.pdf

https://web.mit.edu/curhan/www/docs/Articles/15341_Readings/Justice/Colquitt_Dimensionality_of_Organizational_Justice.pdf

[15] [47] [67] [84] [96] https://dl.acm.org/doi/10.1287/isre.1060.0080

https://dl.acm.org/doi/10.1287/isre.1060.0080

[16] [17] [29] [94] https://ideas.repec.org/a/inm/ororsc/v10y1999i1p104-115.html

https://ideas.repec.org/a/inm/ororsc/v10y1999i1p104-115.html

[18] [73] https://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Science-Privacy-Review.pdf

https://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Science-Privacy-Review.pdf

[22] [34] [103] https://journals.sagepub.com/doi/abs/10.1177/01492063211053224

https://journals.sagepub.com/doi/abs/10.1177/01492063211053224

[23] [42] [44] https://web2-bschool.nus.edu.sg/wp-content/uploads/media_rp/publications/55f7k1423033645.pdf

https://web2-bschool.nus.edu.sg/wp-content/uploads/media_rp/publications/55f7k1423033645.pdf

[25] [39] [41] [61] [70] [85] https://www.jstor.org/stable/258792

https://www.jstor.org/stable/258792

[30] [60] https://www.mckinsey.com/capabilities/quantumblack/our-insights/building-ai-trust-the-key-role-of-explainability

https://www.mckinsey.com/capabilities/quantumblack/our-insights/building-ai-trust-the-key-role-of-explainability

[32] https://selfdeterminationtheory.org/wp-content/uploads/2017/03/2017_DeciOlafsenRyan_annurev-orgpsych.pdf

https://selfdeterminationtheory.org/wp-content/uploads/2017/03/2017_DeciOlafsenRyan_annurev-orgpsych.pdf

[33] [35] [87] https://nissenbaum.tech.cornell.edu/papers/H.%20Nissenbaum%2C%20_Privacy%20as%20Contextual%20Integrity.pdf

https://nissenbaum.tech.cornell.edu/papers/H.%20Nissenbaum%2C%20_Privacy%20as%20Contextual%20Integrity.pdf

[36] https://journals.aom.org/doi/pdf/10.5465/256591

https://journals.aom.org/doi/pdf/10.5465/256591

[37] https://hbr.org/2022/06/monitoring-employees-makes-them-more-likely-to-break-rules

https://hbr.org/2022/06/monitoring-employees-makes-them-more-likely-to-break-rules

[43] [46] [48] [62] [105] https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

[50] https://student.cs.uwaterloo.ca/~cs492/papers/7foundationalprinciples_longer.pdf

https://student.cs.uwaterloo.ca/~cs492/papers/7foundationalprinciples_longer.pdf

[53] https://link.springer.com/article/10.1007/s12525-025-00842-3

https://link.springer.com/article/10.1007/s12525-025-00842-3

[54] [106] https://web-assets.bcg.com/pdf-src/prod-live/a-promise-that-brings-ai-to-life-responsibly.pdf

https://web-assets.bcg.com/pdf-src/prod-live/a-promise-that-brings-ai-to-life-responsibly.pdf

[56] [81] [83] https://www.sciencedirect.com/science/article/pii/S0749597825000172

https://www.sciencedirect.com/science/article/pii/S0749597825000172

[64] https://www.hermanaguinis.com/pdf/BHEPM.pdf

https://www.hermanaguinis.com/pdf/BHEPM.pdf

[69] [91] https://www.sciencedirect.com/science/article/pii/S2451958822000793

https://www.sciencedirect.com/science/article/pii/S2451958822000793

[71] https://pubsonline.informs.org/doi/10.1287/isre.1040.0032

https://pubsonline.informs.org/doi/10.1287/isre.1040.0032

[75] https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work

https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work

[76] [77] https://teddykw2.files.wordpress.com/2012/07/everett-m-rogers-diffusion-of-innovations.pdf

https://teddykw2.files.wordpress.com/2012/07/everett-m-rogers-diffusion-of-innovations.pdf

[86] [97] https://pmc.ncbi.nlm.nih.gov/articles/PMC11300163/

https://pmc.ncbi.nlm.nih.gov/articles/PMC11300163/

[89] [92] https://www.ipc.on.ca/en/media/1826/download?attachment=

https://www.ipc.on.ca/en/media/1826/download?attachment=

[90] https://www.jstor.org/stable/44630759

https://www.jstor.org/stable/44630759

[95] https://misq.umn.edu/misq/article/13/3/319/191/Perceived-Usefulness-Perceived-Ease-of-Use-and

https://misq.umn.edu/misq/article/13/3/319/191/Perceived-Usefulness-Perceived-Ease-of-Use-and

[100] https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters

https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters

[101] https://www.darden.virginia.edu/sites/default/files/inline-files/RaveendhranFast_2021_BehaviorTrackingAcceptance.pdf

https://www.darden.virginia.edu/sites/default/files/inline-files/RaveendhranFast_2021_BehaviorTrackingAcceptance.pdf