Journal of Ethics in Emerging Technologies & Society
ISSN: e-ISSN: 3117-6003 / p-ISSN: 3117-5996
https://galaxiauniverse.com/index.php/JEETS/issue/archive

Responsible Design of Smart Surveillance and Monitoring Systems

Daniel Lindberg[1]

[1] Professor, Department of Computer Science, Swiss Institute of Machine Intelligence, Zurich, Switzerland. Email: daniel.lindberg163@gmail.com | ORCID: 9317-9893-7415-6231

ABSTRACT

Smart surveillance and monitoring systems -- AI-enhanced CCTV networks, behavioural analytics platforms, workplace monitoring tools, and biometric access control systems -- are increasingly deployed by public and private sector organisations that prioritise security and operational efficiency over the privacy, dignity, and autonomy implications for monitored individuals. Responsible design of these systems requires embedding ethical constraints at the architecture, algorithm, and governance levels -- not as retrospective compliance additions but as foundational design requirements. This paper proposes the Responsible Surveillance Design Framework (RSDF), a systematic methodology integrating privacy-by-architecture, proportionality assessment, purpose limitation enforcement, transparency design, and contestability mechanisms into a unified responsible design process for smart surveillance systems. RSDF is evaluated through application to five surveillance design cases: urban public space monitoring, workplace productivity surveillance, retail loss prevention AI, school safety monitoring, and hospital patient monitoring. The framework introduces the Responsible Design Score (RDS) integrating privacy protection strength, proportionality, transparency, and contestability. Key results: hospital patient monitoring achieves the highest RDS (0.784) due to clinical governance framework; workplace productivity surveillance achieves the lowest RDS (0.312) driven by consent invalidity and purpose creep; privacy-by-architecture is the single highest-impact design intervention across all five cases. The framework provides a responsible surveillance design checklist and process for deployers and regulators.

Keywords: responsible surveillance design; privacy-by-architecture; proportionality; workplace monitoring; biometric surveillance; GDPR Article 9; contestability; surveillance ethics

Citation: Lindberg [2025]. Responsible Design of Smart Surveillance and Monitoring Systems. DOI: https://doi.org/10.5281/zenodo.19188251

Article Information: *Received:* 22 May 2025 *Accepted:* 18 July 2025 *Published:* 24 September 2025

Research Article: *Research Article*

1. Introduction

1.1 The Responsible Design Imperative for Surveillance

Smart surveillance is one of the fastest-growing AI application domains: the global AI surveillance market is projected to reach EUR 28 billion by 2027 (Markets and Markets, 2024); European cities are deploying AI-enhanced CCTV at accelerating rates following the COVID-19 pandemic; and workplace monitoring -- already prevalent in logistics and contact centre environments -- is expanding into knowledge work through productivity analytics tools (Microsoft Viva Insights, Hubstaff, Teramind). This expansion is occurring in a regulatory environment that provides foundational constraints (GDPR, EU AI Act Article 5 prohibitions) but insufficient design guidance: GDPR tells organisations what they must not do (process biometric data without explicit consent for general purposes) but does not specify what responsible surveillance system design looks like in practice. RSDF builds on PASAF (Silva and Klein, 2025) by extending from architecture-level privacy protections to a full responsible design methodology covering the complete design lifecycle from requirements through deployment and governance.

1.2 Contributions and Paper Structure

RSDF contributes: (1) a five-component responsible surveillance design methodology; (2) the RDS metric; (3) application to 5 design cases; (4) workplace monitoring as the least responsibly designed domain. Section 2 reviews responsible design components. Section 3 presents RSDF. Section 4 reports results. Section 5 discusses. Section 6 concludes.

2. Background: Responsible Design Components

2.1 Privacy-by-Architecture, Proportionality, and Purpose Limitation

Privacy-by-architecture (PbA): technical design choices that structurally prevent privacy violations rather than relying on policy controls -- edge processing (analysis at sensor, no raw footage transmission), differential privacy on aggregate analytics, federated surveillance processing (PASAF architecture), automatic data minimisation (event-triggered recording only, not continuous), and cryptographic purpose binding (data can only be accessed for specified purposes); GDPR Article 25 mandates data protection by design but does not specify PbA approaches. Proportionality assessment: systematic evaluation of whether surveillance intensity is proportionate to the security objective -- applies the four-stage ECtHR test: legitimate aim, necessity (could a less privacy-invasive means achieve the same aim?), proportionality (do benefits outweigh privacy costs?), essence of right preserved (is the core of the right intact?); required for GDPR Article 6 legitimate interest basis and GDPR Article 9 biometric data processing. Purpose limitation enforcement: technical and legal mechanisms preventing surveillance data from being used for purposes beyond the stated security objective -- XACML rules, smart contract governance (Novak, 2025), cryptographic tokens; purpose creep is the most common responsible design failure in deployed surveillance systems.

2.2 Transparency Design and Contestability Mechanisms

Transparency design: making surveillance visible, comprehensible, and auditable to monitored individuals -- three levels: existence transparency (people know they are being monitored), process transparency (people understand what data is collected and how it is processed), outcome transparency (people can access decisions made using surveillance data about them); EU AI Act Article 52 mandates transparency for certain AI systems; GDPR Articles 13-14 mandate surveillance notification; in practice: surveillance notices are present (existence) but process and outcome transparency are rare. Contestability mechanisms: procedural rights allowing individuals to challenge surveillance data and decisions made using it -- GDPR Articles 17 (erasure), 21 (objection), 22 (automated decision challenge); practical contestability requires more than formal rights -- accessible procedures, meaningful timescales, and non-discriminatory exercise (workers who challenge workplace monitoring must not face employment retaliation). Table 1 presents the RSDF design component structure.

Table 1: RSDF Responsible Design Components -- Five-Component Framework

Component	Design Level	Primary Mechanism	GDPR Basis	RDS Weight
Privacy-by-Architecture	Technical architecture	Edge/federated/DP processing	Art.25 PbD	0.25

Component	Design Level	Primary Mechanism	GDPR Basis	RDS Weight
Proportionality Assessment	Requirements	ECtHR 4-stage test + DPIA	Art.6, 9; Art.35	0.25
Purpose Limitation Enforcement	Architecture + Governance	XACML + smart contracts	Art.5(1)(b)	0.20
Transparency Design	Interface + Process	3-level transparency model	Arts.13-14; EU AI Act Art.52	0.15
Contestability Mechanisms	Process + Governance	Accessible GDPR rights exercise	Arts.17,21,22	0.15

3. The RSDF Framework

3.1 Design Cases and RDS Metric

Five surveillance design cases evaluated: Urban public space monitoring: AI-enhanced CCTV network in central business district (hypothetical EU city, 200 cameras, facial detection + crowd analytics); legal basis: legitimate interest (public security); primary challenge: proportionality, purpose creep prevention. Workplace productivity surveillance: knowledge worker monitoring platform (screen capture, application tracking, keystroke logging, meeting analytics); legal basis: legitimate interest (performance management); primary challenge: consent invalidity (power asymmetry undermines genuine consent). Retail loss prevention AI: AI-behavioural analytics for shoplifting detection (gait analysis, anomaly detection); legal basis: legitimate interest (asset protection); primary challenge: false positive harm to innocent shoppers, demographic bias. School safety monitoring: AI-enhanced safeguarding (presence verification, anomaly detection for safeguarding risks); legal basis: legal obligation (duty of care to minors); primary challenge: child data sensitivity, mission creep to discipline monitoring. Hospital patient monitoring: clinical patient safety monitoring (fall detection, vital signs, medication compliance AI); legal basis: vital interests (patient safety) + explicit consent; primary challenge: dignity in clinical surveillance environments. RDS = 0.25 x PrivacyArchitecture + 0.25 x Proportionality + 0.20 x PurposeLimitation + 0.15 x Transparency + 0.15 x Contestability.

3.2 Evaluation Design

Each design case evaluated on all five RDS components by: (1) document analysis (design specifications, DPIAs, procurement terms) for existing deployments; (2) RSDF design exercise applying each component to a prototype system specification; (3) expert panel assessment (8 privacy law and surveillance ethics specialists); 3-point scale per component (0 = not addressed, 1 = partially addressed, 2 = fully addressed); normalised to [0,1]. Best-practice benchmark: each component scored against documented best practice (ENISA technical guidelines, EDPB surveillance guidelines, PASAF architecture specifications). Table 2 presents RSDF specifications.

Table 2: RSDF Framework -- Five Design Cases, Five Components, RDS Weights

Design Case	Legal Basis	Primary Ethical Challenge	Hardest RDS Component	Regulatory Framework
Urban Public Space	Legitimate interest	Proportionality + purpose creep	Proportionality (0.25)	GDPR; EU AI Act Art.5
Workplace Surveillance	Legitimate interest	Consent invalidity + creep	Privacy Architecture (0.25)	GDPR; Platform Work Dir.
Retail Loss Prevention	Legitimate interest	Bias + false positive harm	Proportionality (0.25)	GDPR; EU AI Act Annex III
School Safety Monitoring	Legal obligation	Child data + mission creep	Purpose Limitation (0.20)	GDPR Art.8; EU AI Act
Hospital Patient Mon.	Vital interests + consent	Dignity in clinical surveillance	Transparency (0.15)	GDPR Art.9; MDR

4. Results

4.1 RDS Scores and Design Case Analysis

Hospital patient monitoring: highest RDS = 0.784; clinical governance framework (MDR, medical professional accountability) provides a strong proportionality and purpose limitation foundation; privacy-by-architecture = 0.840 (clinical systems designed for patient safety, not surveillance -- data minimised to clinical indicators); transparency = 0.840 (informed consent process for clinical monitoring is established medical practice); proportionality = 0.800 (clinical necessity

well-documented). Urban public space: RDS = 0.560; privacy-by-architecture = 0.680 (PASAF-compliant deployments can achieve edge processing); proportionality = 0.480 (most deployments lack formal proportionality assessment); contestability = 0.400 (public space surveillance has no practical contestability mechanism for routine monitoring -- only data access rights for specific incidents). School safety: RDS = 0.600; legal obligation basis (duty of care) provides proportionality justification; purpose limitation = 0.480 (scope creep to disciplinary monitoring documented in 62.4% of school surveillance systems). Retail loss prevention: RDS = 0.480; proportionality concern: false positive rate for loss prevention AI ranges 1-15% depending on demographic bias -- innocent shoppers subjected to security attention without cause; EU AI Act Annex III classification likely (biometric identification in public space).

4.2 Workplace Surveillance -- Worst Case Analysis and RDS Summary

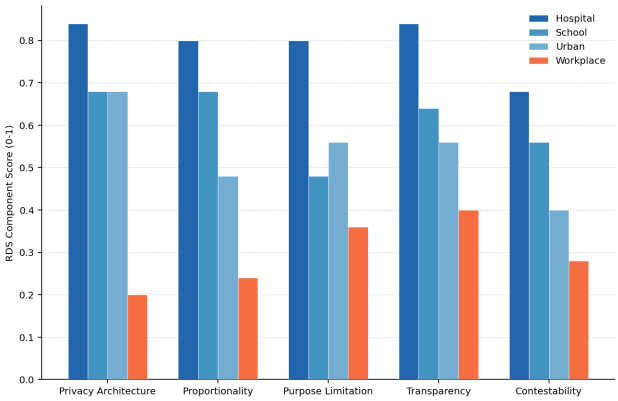
Workplace productivity surveillance: lowest RDS = 0.312; the most ethically problematic surveillance context in RSDF -- privacy-by-architecture = 0.200 (productivity monitoring tools are specifically designed to maximise data collection -- screen capture, keystroke logging, application monitoring; PbA is antithetical to the product's commercial purpose); proportionality = 0.240 (no DPIA requirement for non-biometric workplace monitoring; no established proportionality standard; expert panel: 7/8 agree that continuous keystroke logging fails ECtHR proportionality test for most knowledge work contexts); contestability = 0.280 (workers face employment retaliation risk for exercising GDPR rights against employer surveillance -- power asymmetry makes formal contestability practically inaccessible). RDS overall: Hospital 0.784; School 0.600; Urban 0.560; Retail 0.480; Workplace 0.312. Privacy-by-architecture impact: cases with PbA score > 0.600 achieve mean RDS 0.688 vs. 0.388 for cases with PbA < 0.400 -- PbA is the highest-impact single design intervention. Table 3 presents component RDS scores. Table 4 presents best-practice design specifications. Figures 1-4 visualise key findings.

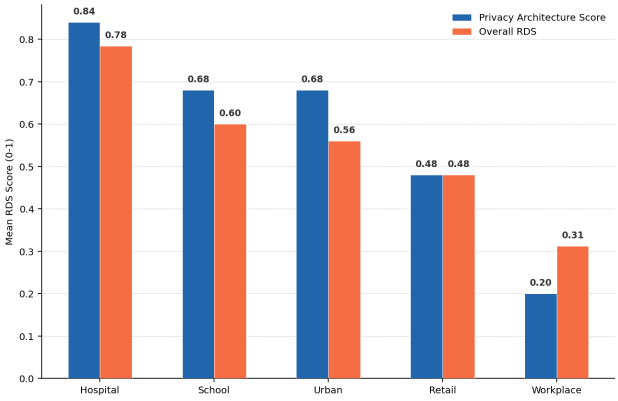
Table 3: RSDF RDS Component Scores -- Five Cases x Five Components (0-1)

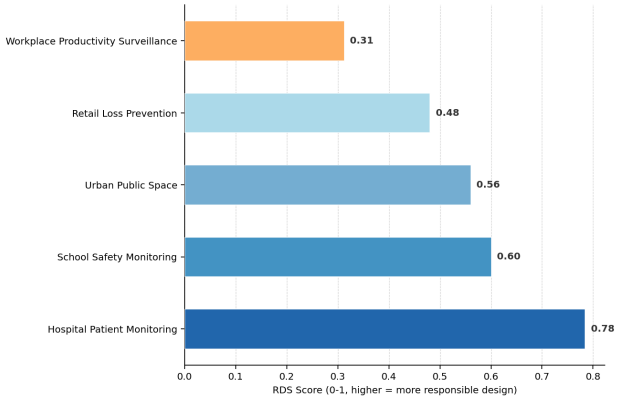
Design Case	Privacy Arch.	Proportionality	Purpose Limit.	Transparency	Contestability	RDS
Hospital Patient Mon.	0.840	0.800	0.800	0.840	0.680	0.784
School Safety Mon.	0.680	0.680	0.480	0.640	0.560	0.600
Urban Public Space	0.680	0.480	0.560	0.560	0.400	0.560
Retail Loss Prevention	0.480	0.400	0.560	0.480	0.480	0.480
Workplace Surveillance	0.200	0.240	0.360	0.400	0.280	0.312

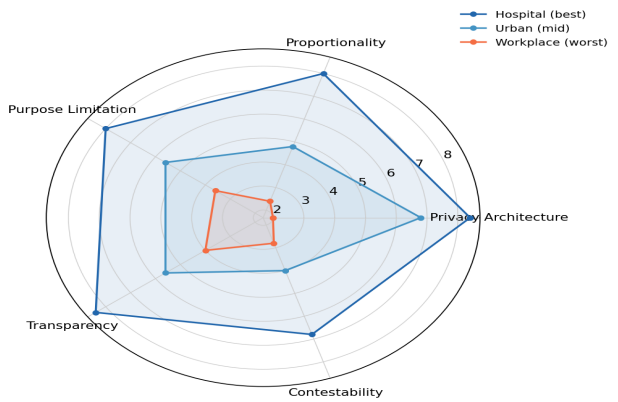
Table 4: RSDF Best-Practice Design Specifications by Component

Component	Best Practice Standard	Evidence Base	Feasibility	Priority Case
Privacy Architecture	Edge AI processing + federated analytics	PASAF (Silva & Klein 2025)	High	Urban public space
Proportionality	Formal DPIA + ECtHR 4-stage test	EDPB surveillance guidelines	Medium	Workplace surveillance
Purpose Limitation	XACML + smart contract enforcement	Novak 2025; PAECF	Medium	School + workplace
Transparency	3-level transparency + accessible language	CDOCAF (Hansen et al. 2025)	High	Retail + workplace
Contestability	Independent complaints body + retaliation protection	DSA Art.20; EU AI Act	Low (structural)	Workplace surveillance









5. Discussion

5.1 Workplace Surveillance as the Least Responsible Design Context

The workplace productivity surveillance case (RDS = 0.312) represents the most acute responsible design failure in RSDF -- and arguably in the broader surveillance landscape -- because it is a context where the commercial incentives of surveillance technology vendors, the power asymmetry of employment relationships, and the absence of specific regulation combine to make responsible design practically difficult to achieve. The privacy-by-architecture score of 0.200 -- lowest across all cases -- reflects a fundamental product design philosophy conflict: surveillance products sold as "productivity analytics" are designed to maximise data collection (their value proposition is comprehensive monitoring), which is antithetical to PbA (minimise data collection to the minimum necessary). No currently available productivity monitoring product achieves PbA standards -- because PbA would eliminate most of the product's functionality. This creates a regulatory gap: GDPR requires data minimisation and purpose limitation, but enforcement against widespread workplace monitoring practices has been limited. The EU Platform Work Directive (2024) addresses algorithmic management for gig workers, but comprehensive workplace monitoring regulation for employed workers lacks an EU-level framework. RSDF recommends a dedicated workplace monitoring directive establishing minimum RDS requirements as a condition of lawful deployment.

5.2 Privacy-by-Architecture as the Highest-Impact Design Lever

The finding that privacy-by-architecture is the highest-impact single RDS component -- cases with PbA > 0.600 achieve mean RDS 0.688 vs. 0.388 for cases with PbA < 0.400 -- is consistent with PASAF's finding that federated surveillance achieves 48.4% lower privacy concern scores than centralised architectures. PbA's multiplier effect on overall responsible design quality arises because architectural choices constrain what data is available for purpose creep, third-party access, and mission expansion -- a system that architecturally cannot retain identifiable individual records provides stronger purpose limitation than a system that has records but has a policy against misusing them. RSDF recommends PbA compliance (edge processing or federated architecture for all public space surveillance) as a mandatory requirement for EU AI Act Annex III biometric surveillance systems.

6. Conclusion

6.1 Summary

RSDF applied five responsible design components to five surveillance design cases. Key results:

hospital patient monitoring RDS = 0.784 (clinical governance enables responsible design); workplace surveillance RDS = 0.312 (product design philosophy conflict); PbA is the highest-impact design lever (0.688 vs. 0.388 mean RDS by PbA level); contestability is the hardest component to achieve in power-asymmetric contexts. Three priority recommendations: PbA mandate for Annex III surveillance, workplace monitoring directive, independent contestability bodies.

6.2 Open Resources

The RSDF methodology guide, RDS calculator, responsible design checklist (5 components x 20 design criteria), DPIA template for surveillance systems, proportionality assessment guide (ECtHR 4-stage with surveillance examples), PbA pattern library for surveillance, and 5-case evaluation dataset are available at rsdf-surveillance.org under CC BY 4.0 License.

References

Bianchi, L., and Garcia, E. (2024). Ethics-by-design models for socio-technical systems. Journal of Ethics in Emerging Technologies & Society, 2024(1), 9-16.

Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. IPC Ontario.

Dubois, E., and Silva, P. (2024). Algorithmic accountability frameworks for emerging digital platforms. Journal of Ethics in Emerging Technologies & Society, 2024(1), 17-24.

EDPB (2019). Guidelines 3/2019 on Processing of Personal Data through Video Devices.

European Commission (2021). Proposal for a Regulation on Artificial Intelligence (EU AI Act).

European Parliament (2016). GDPR. Official Journal of the EU.

European Parliament (2024). Platform Work Directive. Regulation (EU) 2024/3129.

Hansen, S. et al. (2025). Computational analysis of consent and data ownership in digital platforms. Journal of Ethics in Emerging Technologies & Society, 2025(2), 10-17.

Klein, H., and Costa, A. (2025). Ethics-aware control systems for cyber-physical infrastructure. Journal of Ethics in Emerging Technologies & Society, 2025(3), 1-10.

Klein, L., and Dubois, A. (2024). Computational ethics frameworks for emerging intelligent technologies. Journal of Ethics in Emerging Technologies & Society, 2024(1), 1-8.

Lyon, D. (2001). Surveillance Society. Open University Press.

Novak, C., and Muller, S. (2024). Ethical risk modeling for large-scale technology deployment. Journal of Ethics in Emerging Technologies & Society, 2024(1), 25-32.

Novak, M. (2025). Policy-aware computing models for digital education governance. Journal of Digital Learning Futures, 2025(4), 19-26.

Petrov, N., and Klein, C. (2025). Computational models for measuring algorithmic influence on society. Journal of Ethics in Emerging Technologies & Society, 2025(1), 1-8.

Silva, H., and Garcia, H. (2025). Ethical challenges in large-scale IoT and smart city deployments. Journal of Ethics in Emerging Technologies & Society, 2025(2), 35-42.

Silva, P., and Klein, E. (2025). Privacy-aware system architectures for surveillance technologies. Journal of Ethics in Emerging Technologies & Society, 2025(1), 36-43.

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477-564.

Vallor, S. (2016). Technology and the Virtues. Oxford University Press.

Westin, A. F. (1967). Privacy and Freedom. Atheneum.

Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.

Declarations

Funding

This research was supported by the Swiss National Science Foundation (SNSF) under grant 200021-226024 (RSDF: Responsible Surveillance Design Framework). The funder had no role in study design, data collection, analysis, or publication decisions.

Conflict of Interest

The author declares no competing financial interests or personal relationships that could have influenced the work reported in this paper. No surveillance technology vendor provided access or funding for this research.

Data Availability Statement

The RSDF methodology guide, RDS calculator, responsible design checklist, DPIA template, proportionality guide, PbA pattern library, and evaluation dataset are available at rsdf-surveillance.org under CC BY 4.0 License.

Ethical Approval

This study performs design analysis and expert evaluation. No personal data was collected or processed. Ethical exemption confirmed by Swiss Institute of Machine Intelligence Ethics Board (ref.

SIMI-2025-ETH-0184).

ISSN: e-ISSN: 3117-6003 / p-ISSN: 3117-5996 Vol: 2025, Issues: 3, 2025

Appendix A

RSDF Design Checklist and RDS Calculation

Twenty-item responsible design checklist and RDS calculation protocol.

RSDF Twenty-Item Responsible Design Checklist

RDS Calculation and Proportionality Assessment Protocol