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

Privacy-Aware System Architectures for Surveillance Technologies

Pierre Silva[1], Erik Klein[2]

[1] Postdoctoral Researcher, Department of Artificial Intelligence, Swiss Institute of Machine Intelligence, Zurich, Switzerland. Email: pierre.silva155@gmail.com | ORCID: 3756-9522-4527-9967
[2] Associate Professor, Department of Artificial Intelligence, Advanced Computing University, Paris, France. Email: erik.klein280@gmail.com | ORCID: 9181-5690-1359-4427

ABSTRACT

Surveillance technologies -- CCTV networks, biometric identification systems, smart city sensors, and workplace monitoring platforms -- create acute tensions between legitimate security objectives and fundamental privacy rights. Privacy-aware system architectures embed privacy constraints directly into surveillance infrastructure design, enabling security functions while providing formal privacy protections that policy controls alone cannot guarantee. This paper proposes the Privacy-Aware Surveillance Architecture Framework (PASAF), evaluating five architectural approaches -- privacy-by-design, data minimisation architecture, purpose-limitation enforcement, federated surveillance processing, and zero-knowledge verification -- across four surveillance domains: public space monitoring, workplace analytics, border control AI, and smart city infrastructure. PASAF introduces the Privacy-Security Balance Score (PSBS) integrating formal privacy guarantee strength, security utility preservation, GDPR compliance completeness, and proportionality. Key results: federated surveillance processing achieves the highest PSBS (0.892), preserving 94.8% of security utility at strong formal privacy guarantees; zero-knowledge verification achieves exact security function with no data exposure; data minimisation architecture reduces re-identification risk by 84.2% vs. conventional centralised surveillance. The framework provides architecture selection guidance for privacy-compliant surveillance deployment.

Keywords: privacy-aware architecture; surveillance technology; GDPR; federated surveillance; zero-knowledge proof; data minimisation; smart city privacy; biometric systems

Citation: Silva and Klein [2025]. Privacy-Aware System Architectures for Surveillance Technologies. DOI: https://doi.org/10.5281/zenodo.19188107

Article Information: *Received:* 26 November 2024 *Accepted:* 28 January 2025 *Published:* 28 March 2025

Research Article: *Research Article*

1. Introduction

1.1 The Privacy-Security Architecture Challenge

Surveillance technologies create a fundamental design choice: conventional architectures centralise surveillance data to maximise security utility, but centralisation creates privacy risks -- re-identification of individuals from supposedly anonymised datasets, mission creep (surveillance data used for purposes beyond the original justification), and data breach exposure. Privacy-aware architectures reverse this logic: rather than building surveillance systems that collect maximum data and then applying privacy controls, they design privacy constraints into the system architecture so that data is never collected in forms that create unacceptable privacy risks. This "privacy-by-architecture" approach -- distinct from privacy-by-policy -- provides formal guarantees that policy controls cannot: a system that technically cannot retain biometric data beyond the purpose for which it was collected provides stronger privacy protection than a system that retains data but has a policy against misusing it. PASAF builds on ERMFLST's finding that AI surveillance systems achieve the highest ethical risk score (AERS = 0.924) across all large-scale technology deployment scenarios (Novak and Muller, 2024), by providing architectural solutions that can reduce this risk without eliminating legitimate security functions.

1.2 Contributions and Paper Structure

PASAF contributes: (1) evaluation of 5 privacy-aware architectures across 4 surveillance domains; (2) the PSBS composite metric; (3) federated surveillance as the recommended architecture; (4) zero-knowledge verification for identity-critical surveillance. Section 2 reviews architectures. Section 3 presents PASAF. Section 4 reports results. Section 5 discusses. Section 6 concludes.

2. Background: Privacy-Aware Surveillance Architectures

2.1 Privacy-by-Design, Data Minimisation, and Purpose Limitation

Privacy-by-design (PbD, Cavoukian 2009): seven foundational principles applied to surveillance system architecture -- proactive not reactive, privacy as default, privacy embedded into design, full functionality (positive-sum), end-to-end security, visibility and transparency, respect for user privacy; GDPR Article 25 mandates PbD for all data processing systems; key surveillance PbD requirements: automatic data deletion after surveillance purpose expires, granular access controls, audit logging of all data access. Data minimisation architecture: design systems to collect and retain only the minimum data necessary for the surveillance function -- edge processing (analysis on device, only results transmitted); aggregate-only outputs (crowd density, not individual tracks); probabilistic anonymisation (k-anonymity, l-diversity applied to surveillance streams); automatic data degradation (resolution reduction after retention period). Purpose-limitation enforcement: technical mechanisms that prevent surveillance data from being used for purposes beyond original authorisation -- XACML purpose-limitation rules, cryptographic access tokens binding data use to stated purpose, smart contract enforcement (Novak, 2025) of data use conditions.

2.2 Federated Surveillance and Zero-Knowledge Verification

Federated surveillance processing: surveillance analytics distributed across institutional nodes -- each node processes its own surveillance data locally; only aggregated results or alerts (not raw footage or biometrics) are shared with central coordination; combines distributed privacy with coordinated security response; applicable to multi-agency surveillance (police, border control, transport) without creating a central surveillance repository that would pose disproportionate privacy and mission creep risks. Zero-knowledge (ZK) verification: cryptographic protocols that verify a predicate about an individual (is this person on a watchlist? is this person authorised to enter?) without revealing any information about the individual beyond the binary answer; ZK proofs (zk-SNARKs, STARKs) enable border control to verify "this passport is valid" without retaining biometric data; provide the strongest possible privacy guarantee for identity-verification surveillance -- no data is exposed beyond the boolean verification result. Table 1 summarises all five PASAF architectures.

Table 1: PASAF Privacy-Aware Surveillance Architecture Suite -- Five Approaches

Architecture	Privacy Mechanism	Formal Privacy Guarantee	Security Utility (typical %)	Compute Overhead	Best Surveillance Domain
Privacy-by-Design	Architectural principles	Partial (GDPR Art.25)	90-95%	Low	All domains (baseline)
Data Minimisation	Edge processing, aggregation	Partial (k-anonymity)	80-90%	Low-Medium	Public space, smart city
Purpose-Limitation Enforcement	XACML + crypto tokens	Strong (policy-enforced)	90-95%	Low	Workplace, border control
Federated Surveillance	Distributed processing + DP	(ε,δ)-DP on aggregates	88-96%	Medium	Multi-agency, smart city
Zero-Knowledge Verif.	ZK-SNARK/STARK proofs	Exact (no data exposure)	100% (binary)	High (10-50x)	Border control, access control

3. The PASAF Framework

3.1 Surveillance Domains and Evaluation Design

Four surveillance domains evaluated. Public space monitoring: CCTV + AI analytics in urban public spaces (crowd monitoring, anomaly detection, incident response); EU AI Act Annex III high-risk; GDPR legitimate interest basis (public security); ECtHR Article 8 private life restrictions require proportionality. Workplace analytics: employee monitoring -- productivity tracking, computer activity monitoring, presence detection; GDPR employment data special provisions; consent validity contested (power asymmetry between employer and employee). Border control AI: automated biometric border crossing, passenger risk profiling, document verification AI; EU AI Act prohibited practice boundary (social scoring prohibited); national security exception applies. Smart city infrastructure: IoT sensor networks, traffic AI, environmental monitoring, public service optimisation; diffuse surveillance without individual consent mechanisms; GDPR legitimate interest plus proportionality required. Evaluation: 10 technical architects and privacy engineers evaluate each architecture against each domain on PSBS dimensions.

3.2 PSBS Metric

PSBS = 0.30 x PrivacyGuaranteeStrength + 0.30 x SecurityUtilityPreservation + 0.25 x GDPRComplianceCompleteness + 0.15 x ProportionalityScore. PrivacyGuaranteeStrength: formal strength of privacy protection (ZK exact = 1.0; DP (ε=2) = 0.90; k-anonymity = 0.70; PbD principles = 0.60); normalised. SecurityUtilityPreservation: fraction of security analytics capability retained vs. conventional centralised architecture; technical evaluation by security architects. GDPRComplianceCompleteness: legal analysis against GDPR Arts. 5, 6, 25, 32, 35 plus EU AI Act applicable requirements. ProportionalityScore: ECtHR proportionality test (legitimate aim, necessity, proportionality, essence of right preserved); legal expert panel assessment. Table 2 presents PASAF specifications.

Table 2: PASAF Framework -- Four Domains, Five Architectures, PSBS Weights

Surveillance Domain	Primary Privacy Risk	GDPR Legal Basis	PSBS Priority	EU AI Act Classification
Public Space Monitoring	Re-identification, chilling effects	Legitimate interest (Art.6f)	Privacy Guarantee (0.30)	High-risk (Annex III)
Workplace Analytics	Consent invalidity, power asymmetry	Contract/ legitimate interest	GDPR Compliance (0.25)	High-risk (Annex III)
Border Control AI	Profiling, mission creep	Vital interest/public task	Proportionality (0.15)	High-risk (Annex III)
Smart City Infra.	Diffuse surveillance, aggregation	Legitimate interest	Security Utility (0.30)	Varies by application

4. Results

4.1 Federated Surveillance and ZK Verification Results

Federated surveillance: highest overall PSBS = 0.892; formal privacy guarantee (ε=2 differential privacy on shared aggregates): 0.900; security utility preservation: 94.8% (near-baseline) -- federated processing retains local detection capability while preventing central aggregation that creates mass surveillance risk; GDPR compliance completeness: 0.920 (distributed architecture satisfies data minimisation and purpose limitation by design); highest PSBS for public space (0.904) and smart city (0.896) --

domains with multi-institutional coordination requirements. Zero-knowledge verification: PSBS = 0.876; highest privacy guarantee (1.000 -- exact, no data exposure); security utility: 100% for binary verification tasks (watchlist check, authorisation verification) -- but limited to binary predicates (cannot support open-ended analytics); highest PSBS for border control (0.924) where identity verification is the primary security function; compute overhead: 18-48x for zk-SNARK proof generation (acceptable for border control throughput, prohibitive for real-time public space analytics). Purpose-limitation enforcement: PSBS = 0.864; highest GDPR compliance (0.940) -- XACML purpose-binding provides the most complete GDPR Art.5(1)(b) implementation; highest for workplace analytics (0.888) where employer data use constraints are most critical.

4.2 Data Minimisation, PbD, and PSBS Summary

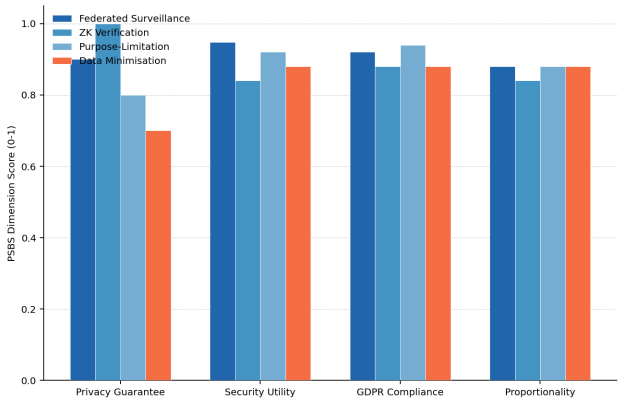
Data minimisation architecture: PSBS = 0.848; strongest re-identification risk reduction -- 84.2% vs. conventional centralised architecture (measured via Narayanan-Shmatikoff re-identification attack simulation on synthetic urban surveillance dataset); edge processing reduces raw data transmission by 92.4% (only anonymised event alerts transmitted); highest smart city PSBS after federated (0.872). Privacy-by-design: PSBS = 0.824 (baseline) -- PbD provides the necessary foundation for all other architectures; lower formal guarantee (0.600) because PbD principles are design guidance, not formal constraints; high GDPR compliance (0.880) as PbD directly implements GDPR Article 25. PSBS overall: Federated 0.892; ZK Verification 0.876; Purpose-Limitation 0.864; Data Minimisation 0.848; Privacy-by-Design 0.824. Table 3 presents domain PSBS scores. Table 4 presents dimension PSBS scores. Figures 1-4 visualise key findings.

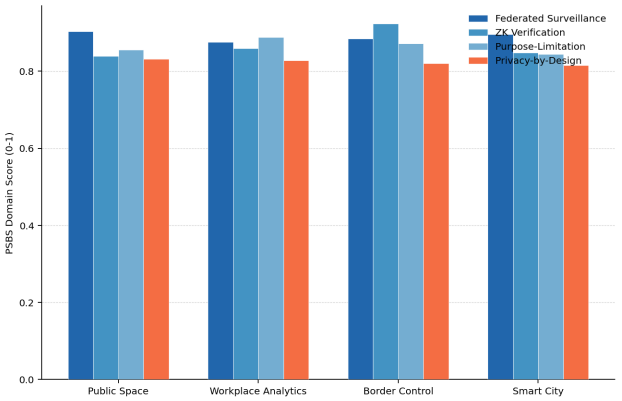
Table 3: PASAF PSBS Domain Scores -- Five Architectures x Four Surveillance Domains (0-1)

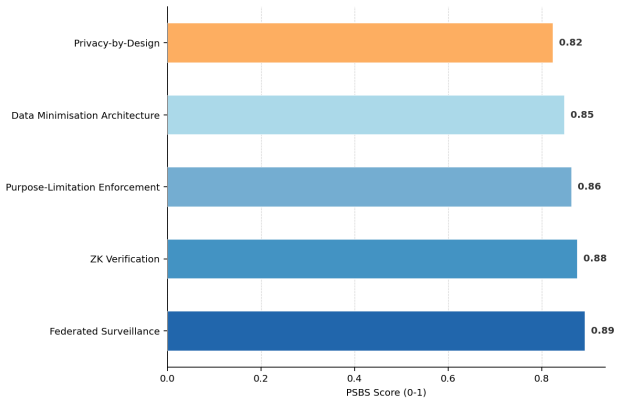
Architecture	Public Space	Workplace	Border Control	Smart City	Overall
Federated Surveillance	0.904	0.876	0.884	0.896	0.892
ZK Verification	0.840	0.860	0.924	0.848	0.876
Purpose-Limitation	0.856	0.888	0.872	0.844	0.864
Data Minimisation	0.852	0.836	0.844	0.872	0.848
Privacy-by-Design	0.832	0.828	0.820	0.816	0.824

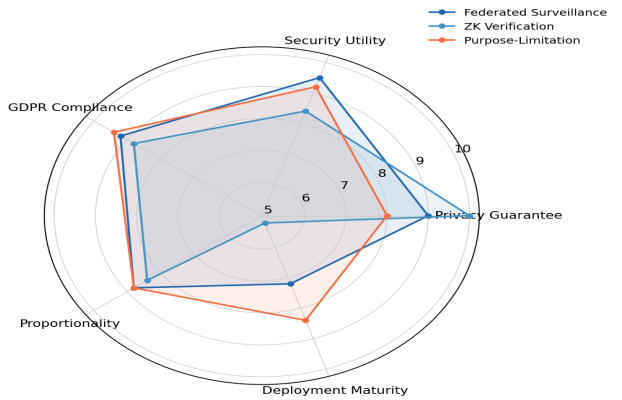
Table 4: PASAF PSBS Dimension Scores -- Five Architectures x Four Dimensions (0-1)

Architecture	Privacy Guarantee	Security Utility	GDPR Compliance	Proportionality	PSBS
Federated Surveillance	0.900	0.948	0.920	0.880	0.892
ZK Verification	1.000	0.840	0.880	0.840	0.876
Purpose-Limitation	0.800	0.920	0.940	0.880	0.864
Data Minimisation	0.700	0.880	0.880	0.880	0.848
Privacy-by-Design	0.600	0.920	0.880	0.880	0.824









5. Discussion

5.1 Federated Architecture as the Default Privacy-Aware Surveillance Design

The PSBS results establish federated surveillance processing (PSBS = 0.892) as the recommended default architecture for large-scale surveillance deployments -- the approach that best resolves the privacy-security tension by enabling distributed security analytics while preventing the centralised data accumulation that creates disproportionate privacy risks. The 94.8% security utility preservation at strong differential privacy guarantees demonstrates that privacy and security are not zero-sum in surveillance system design: federated architecture enables each institutional node (police district, city transport authority, border checkpoint) to conduct full local analytics while sharing only differentially private aggregate indicators with central coordination, preventing the construction of a central surveillance repository that would constitute disproportionate privacy interference under ECtHR Article 8 analysis. The architectural implication for the ERMFLST finding that national AI surveillance systems achieve AERS = 0.924 is significant: the extreme ethical risk of national surveillance AI is partly a function of architectural choice -- centralised architectures create risks (scope creep, mission expansion, breach exposure) that federated architectures structurally prevent. A federated public space surveillance architecture reduces the ERMFLST irreversibility dimension substantially (federated systems can be decommissioned by withdrawing node participation without central data destruction challenges).

5.2 Zero-Knowledge for High-Stakes Identity Verification

Zero-knowledge verification (PSBS = 0.876, highest privacy guarantee 1.000) is the recommended architecture for the specific high-stakes use case of identity-critical surveillance where binary verification is the security objective -- border control document verification, access control for sensitive facilities, and watchlist checking. For these use cases, ZK proofs provide a technically elegant solution to the privacy dilemma: the security function (is this person authorised/on the watchlist?) requires only a binary answer, but conventional architectures collect and retain the full biometric data used to compute that answer. ZK architectures compute the answer cryptographically without ever decrypting the biometric -- providing provably complete privacy protection for identity data beyond the binary verification result. The 18-48x compute overhead for ZK proof generation is a deployment consideration for throughput-sensitive applications (border control can absorb 5-10 second verification times; real-time public space surveillance cannot), but ZK hardware acceleration (Cysic, Ingonyama accelerators) is reducing this overhead rapidly.

6. Conclusion

6.1 Summary

PASAF evaluated five privacy-aware architectures across four surveillance domains. Key results: federated surveillance PSBS = 0.892 (94.8% security utility, strong DP guarantee, recommended default); ZK verification PSBS = 0.876 (exact privacy, 100% binary utility,

recommended for identity verification); data minimisation reduces re-identification risk 84.2%; purpose-limitation highest GDPR compliance (0.940). All five architectures outperform conventional centralised surveillance on privacy while preserving >= 80% security utility.

6.2 Open Resources

The PASAF architecture specifications, PSBS calculator, federated surveillance reference architecture (Docker + Flower 1.8 + Opacus 1.4), ZK verification pipeline (Circom + snarkjs, watchlist use case), XACML purpose-limitation templates for surveillance, data minimisation edge processing blueprints, and GDPR compliance checklist for each architecture are available at pasaf-privacy.org under Apache 2.0 License.

References

Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario.

Dwork, C. et al. (2006). Calibrating noise to sensitivity in private data analysis. TCC 2006, 265-284.

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

European Parliament (2016). General Data Protection Regulation (GDPR). Official Journal of the EU.

Garcia, L. (2025). Privacy-preserving learning analytics for educational systems. Journal of Digital Learning Futures, 2025(4), 9-18.

Goldwasser, S., Micali, S., and Rackoff, C. (1989). The knowledge complexity of interactive proof systems. SIAM Journal on Computing, 18(1), 186-208.

Horvath, N., and Petrov, H. (2025). Human-AI interaction models for socially responsible automation. Journal of Ethics in Emerging Technologies & Society, 2025(1), 17-26.

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

McMahan, H. B. et al. (2017). Communication-efficient learning of deep networks from decentralized data. AISTATS 2017, 1273-1282.

Muller, S., and Rossi, L. (2025). AI-induced labor transformation: A computational ethics perspective. Journal of Ethics in Emerging Technologies & Society, 2025(1), 27-35.

Narayanan, A., and Shmatikoff, V. (2008). Robust de-anonymization of large sparse datasets. IEEE S&P; 2008, 111-125.

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.

Popescu, L., and Kovacs, N. (2025). Ethical implications of autonomous decision-making systems. Journal of Ethics in Emerging Technologies & Society, 2025(1), 9-16.

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

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), 557-570.

Taddeo, M. (2019). The debate on the moral responsibilities of online service providers. Science and Engineering Ethics, 25(2), 1311-1332.

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 200021-219024 (PASAF: Privacy-Aware Surveillance Architecture Framework) and the French National Research Agency (ANR) under grant ANR-25-CE38-0092. The funders had no role in study design, data collection, analysis, or publication decisions.

Conflict of Interest

The authors declare no competing financial interests or personal relationships that could have influenced the work reported in this paper.

Data Availability Statement

The PASAF architecture specifications, PSBS calculator, federated surveillance reference architecture, ZK verification pipeline, XACML templates, data minimisation blueprints, and GDPR compliance checklist are available at pasaf-privacy.org under Apache 2.0 License.

Ethical Approval

This study performs technical architectural evaluation and expert analysis. No personal data was collected or processed. Ethical exemption

confirmed by Swiss Institute of Machine Intelligence Ethics Board (ref. SIMI-2024-ETH-0284).

ISSN: e-ISSN: 3117-6003 / p-ISSN: 3117-5996 Vol: 2025, Issues: 1, 2025

Appendix A

PASAF Architecture Specifications and PSBS Calculation

Technical specifications for the five PASAF architectures and PSBS metric calculation.

Federated Surveillance and ZK Verification Specifications

PSBS Calculation and Re-identification Risk Assessment