

Balancing Privacy and State Surveillance: A Comparative Study of Necessity, Proportionality and Accountability

Pawan Bindal, Dr. Ramveer Singh

Ph.D. scholar, MVN University, Palwal, Haryana, India 121105

Email Id: pawanbindal1800@gmail.com

Associate Professor, MVN University, Palwal, Haryana, India 121105

Email Id: ramveer.singh@mvn.edu.in

HOW TO CITE: ABSTRACT:

Pawan Bindal, Ramveer Singh
(2026). Balancing Privacy and State
Surveillance:
A Comparative Study of Necessity,
Proportionality and Accountability.
International Journal of Special
Education, 41(23s), 1384 - 1406

The rapid expansion of administrative surveillance has fundamentally altered the relationship between the individual and the State, creating complex tensions between the imperatives of governance and the protection of individual privacy. Technological developments in artificial intelligence, biometric identification, predictive analytics, facial recognition, data mining, and digital monitoring have significantly enhanced the State's capacity to collect, process, correlate, and retain personal information. While surveillance may serve legitimate objectives such as national security, prevention of crime, public safety, and efficient administration, its unchecked or inadequately regulated use raises profound concerns regarding informational autonomy, dignity, liberty, anonymity, and the possibility of arbitrary State intrusion.

This paper critically examines the contemporary resilience of the right to privacy in the context of expanding administrative surveillance through a comparative legal framework. It analyses the constitutional and statutory safeguards governing surveillance in India, with particular emphasis on the transformative recognition of privacy as a constitutionally protected right in Justice K.S. Puttaswamy (Retd.) v. Union of India. The study further examines comparative jurisprudence, including *Carpenter v. United States*, alongside relevant developments before the European Court of Human Rights and international human rights institutions, to identify emerging standards governing State access to personal data and digital information.

The paper evaluates whether existing legal frameworks are sufficiently equipped to address technologically sophisticated forms of surveillance. Particular attention is given to the principles of legality, legitimate aim, necessity, proportionality, procedural safeguards, independent oversight, transparency, accountability, and effective remedies. It argues that the mere existence of a statutory framework cannot, by itself, ensure

meaningful protection of privacy unless surveillance powers are subjected to substantive and procedural limitations capable of responding to contemporary technological realities. A descriptive reanalysis of the twelve-authority corpus yields 78 reported engagements across 96 possible safeguard cells (81.25%); transparency appears in five authorities (41.67%). Technical sensitivity analyses connect proportionality to location sampling, base-rate error, query geometry and retained data volume, with simulated quantities explicitly distinguished from observed evidence.

The study further contends that the future of privacy protection requires a shift from reactive judicial intervention towards a comprehensive privacy-conscious governance architecture. Strengthening independent oversight, judicial and parliamentary scrutiny, data-minimisation standards, transparency obligations, accountability mechanisms, and effective remedies can help reconcile legitimate administrative objectives with constitutional commitments to privacy and individual liberty. The paper ultimately proposes a rights-based approach to administrative surveillance in which technological capability is balanced by legal restraint, ensuring that the pursuit of collective security does not result in the erosion of individual autonomy and constitutional freedom.

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the
terms and conditions
of the Creative Commons Attribution
(CC BY)
license (<http://creativecommons.org/licenses/by/4.0/>).

Keywords: Right to Privacy, Administrative Surveillance, Informational Privacy, Constitutional Rights, Proportionality, Necessity, Artificial Intelligence, Biometric Surveillance, Data Protection, Digital Governance, State Surveillance.

1. Introduction

The contemporary surveillance state is increasingly defined by data integration rather than by a single act of observation. Traditional interception targeted a telephone line, a letter or a particular communication. Contemporary systems can combine location histories, biometric identifiers, communications metadata, facial images, financial or administrative records, network relationships and behavioural predictions. The legal significance of this shift is substantial: surveillance can become continuous, inferential and population-scale even when each individual data point appears ordinary in isolation.

The central constitutional problem is the justification and control of State access to personal data. Surveillance may pursue legitimate objectives including national security, prevention of crime, public safety and efficient administration, but technological capability can also undermine

informational autonomy, dignity, liberty and anonymity when collection is indiscriminate or insufficiently controlled. The doctrinal question is therefore not whether the State may ever surveil. The more difficult question is how law should determine when surveillance is justified, how intrusive it may be, who should authorize it, how long data may be retained, and what forms of oversight and remedy are necessary when the surveillance is secret.

India provides an especially important setting for this inquiry. The Supreme Court's nine-judge decision in Justice K.S. Puttaswamy (Retd.) v. Union of India recognized privacy as intrinsic to liberty, dignity and autonomy and established that State intrusions require legal authority, a legitimate aim and proportionality, together with safeguards against abuse. Earlier, *PUCL v. Union of India* had described telephone tapping as a serious invasion of privacy and imposed procedural safeguards on executive interception. The present statutory

landscape now includes section 20 of the Telecommunications Act, 2023, the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, section 69 of the Information Technology Act, 2000, the 2009 interception rules, and the Digital Personal Data Protection Act, 2023 with the Digital Personal Data Protection Rules, 2025.¹

Comparative law shows parallel adaptation. In *Carpenter v. United States*, the United States Supreme Court held that acquisition of historical cell-site location information generally constitutes a Fourth Amendment search requiring a warrant supported by probable cause. In *Chatrue v. United States*, decided on 29 June 2026, the Court held that police acquisition of Google Location History through a geofence process was a Fourth Amendment search and remanded the question whether the warrant satisfied probable-cause and particularity requirements at each stage. The European Court of Human Rights has developed a different but convergent body of doctrine requiring foreseeability, necessity, safeguards against abuse, independent authorization or supervision and effective ex post review, particularly in *Roman Zakharov*, *Big Brother Watch* and *Centrum för rättvisa*.²

This paper therefore treats privacy protection as a problem of surveillance-system design. It compares constitutional tests, statutory structures and institutional safeguards, then translates those legal principles into an operational governance model capable of addressing AI-assisted and data-intensive surveillance.

2. Research Problem, Questions And Objectives

The research problem is the widening gap between the scale and inferential power of modern surveillance technologies and legal frameworks that were often designed for discrete interception events. A surveillance regime may have a statutory basis yet still create constitutional risk if authorization is broad, oversight is internal, data collection is excessive, retention is indefinite, or the

affected person lacks any realistic means of challenge.

2.1 Research Questions

1. How do Indian constitutional and statutory rules structure the legality, necessity, proportionality and accountability of State surveillance?
2. What safeguards have the United States Supreme Court and the European Court of Human Rights developed for location data, digital devices, secret interception and bulk surveillance?
3. Which safeguards recur most consistently across leading authorities, and where do institutional models materially diverge?
4. How should legal controls be redesigned for AI-enabled, biometric, predictive, geolocation and data-fusion surveillance?

2.2 Objectives

1. To map the contemporary surveillance-law framework in India, including telecommunications interception, computer-resource interception and data-protection rules.
2. To compare Indian privacy doctrine with United States Fourth Amendment jurisprudence and European human-rights standards.
3. To conduct a structured doctrinal content analysis of selected leading authorities using a transparent safeguard-coding protocol.
4. To formulate a technology-neutral but risk-sensitive governance model based on legality, legitimate aim, necessity, proportionality, minimization, independent oversight, accountability and effective remedy.

3. Literature Review And Research Gap

Privacy scholarship has long warned that surveillance harm is not confined to secrecy or disclosure. Surveillance can alter behaviour, concentrate institutional power, enable categorisation and exclusion, and chill association or expression even when collected information is never publicly released. Daniel Solove's taxonomy of privacy and Neil Richards' work on intellectual privacy and surveillance help explain why data aggregation can produce harms different from those associated with a single disclosure. Julie

¹ Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1. (1997) 1 SCC 301 (judgment dated Dec. 18, 1996). The Telecommunications Act, 2023 (Act 44 of 2023), s. 20(2).

² 585 U.S. 296 (2018). 609 U.S. (2026), No. 25-112, slip opinion (June 29, 2026), available at: https://www.supremecourt.gov/opinions/25pdf/25-112_0am4.pdf (last visited on Sept. 30, 2026).

Cohen's account of informational capitalism further demonstrates how data infrastructures reshape practical autonomy by making individuals continuously legible to institutions.³

Public-law literature has increasingly moved from a binary privacy-versus-security frame toward a governance frame. The key question is whether surveillance power is bounded *ex ante* and reviewable *ex post*. This shift is visible in international human-rights materials, especially the Office of the United Nations High Commissioner for Human Rights report on the right to privacy in the digital age (A/HRC/51/17, 2022), which emphasizes legality, necessity, proportionality, oversight and effective remedies in data-intensive surveillance environments.⁴

Indian literature after Puttaswamy has focused heavily on the constitutionalisation of informational privacy and the adequacy of data-protection legislation. A recurring concern is that ordinary data-protection law and surveillance authorization law perform different functions. Data-protection legislation regulates processing relationships, while surveillance law authorizes coercive State access. The Digital Personal Data Protection Act, 2023 is therefore relevant to surveillance but does not replace the need for independent constitutional scrutiny of interception,

monitoring, decryption, biometric matching or intelligence collection.⁵

The comparative research gap lies in connecting doctrinal tests to technical surveillance architecture. Legal writing often discusses proportionality at a high level, while technical systems make concrete choices about selectors, databases, retention, matching thresholds, query permissions, audit logs and human review. Conversely, technical discussions may emphasize system performance without translating privacy doctrine into design constraints. This paper bridges that gap by coding legal authorities for recurring safeguards and converting those safeguards into a lifecycle governance model.

4. Conceptual And Technical Framework Of State Surveillance

4.1 A Functional Taxonomy of Surveillance Technologies

The legal analysis benefits from distinguishing surveillance by function rather than by device. A function-based taxonomy remains useful even when technologies converge or are replaced. Six categories recur in contemporary administrative surveillance: identification, communications interception, location tracking, behavioural prediction, database fusion, and persistent observation.

Table 1. Technical taxonomy of surveillance modalities and principal legal risks

Surveillance modality	Typical technical function	Primary privacy risk	Minimum legal control
Biometric identification	Face, fingerprint, iris or other biometric matching	Persistent identification; false association; function creep	Clear statutory purpose; necessity; accuracy governance; access controls; retention limits
Communications interception	Capture or disclosure of message content or metadata	Intrusion into confidential communications and associations	Defined triggers; written reasons; authorization; time limits; secure handling; review

³ Daniel J. Solove, "A Taxonomy of Privacy" 154 *University of Pennsylvania Law Review* 477 (2006).
Neil M. Richards, "The Dangers of Surveillance" 126 *Harvard Law Review* 1934 (2013).

⁴ United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/51/17 (Aug. 4, 2022).

⁵ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 17; the Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, sec. 3(i), Nov. 13, 2025, r. 1(2).

Location / geofence surveillance	Historic or real-time device location and area-based queries	Reconstruction of movements; inference of home, religion, health or association	Particularity; probable cause or equivalent necessity; minimization; query logging
Predictive analytics	Risk scoring or prediction from historical and real-time data	Opacity, proxy discrimination, feedback loops and pre-emptive intervention	Explainability appropriate to use; validation; human review; contestability
Data mining / data fusion	Correlation of multiple administrative or commercial datasets	Purpose expansion; hidden profiles; population-scale inference	Purpose limitation; query authorization; minimization; access segmentation; audits
Persistent visual monitoring	CCTV, drones, body-worn systems, AI-assisted video analytics	Continuous observation and automated tracking in public or semi-public spaces	Spatial and temporal limits; notice where feasible; masking; retention and deletion rules

4.2 From “Collection” to the Surveillance Lifecycle

A modern surveillance operation should be treated as a lifecycle with legally relevant stages: acquisition, filtering, enrichment, analysis, sharing, retention, secondary use and deletion. The privacy intrusion may intensify after initial collection because later stages convert raw data into identity, relationship or behavioural inference. This explains the European Court of Human Rights’ emphasis on “end-to-end safeguards” in bulk interception and supports a similar approach for AI-driven administrative surveillance.⁶

4.3 Operationalising Necessity and Proportionality

Necessity should require more than usefulness. The authority should demonstrate a concrete objective, a rational connection between the surveillance method and that objective, and the absence of an equally effective but materially less intrusive alternative. Proportionality in the strict sense then compares the expected public benefit with the scale, sensitivity, duration, identifiability and

downstream uses of the data. This paper treats minimization, independent authorization, auditing and effective review as mechanisms that make proportionality operational rather than rhetorical.⁷

5. Research Methodology

The study adopts a comparative doctrinal and structured legal-content-analysis method. Primary sources include constitutional provisions, statutes, subordinate legislation and reported judicial decisions. Official materials from the Supreme Court of India, the United States Supreme Court, the European Court of Human Rights, India Code, the Department of Telecommunications, the Ministry of Electronics and Information Technology, EUR-Lex and the United Nations are prioritized.⁸

For the comparative component, twelve authorities were purposively selected across India, the United States and the European Court of Human Rights, with four authorities in each group. Eight safeguards are summarized as reported engagement counts. The quantitative analysis treats these aggregate counts as descriptive doctrinal indicators,

⁶ *Big Brother Watch and Others v. the United Kingdom [GC]*, Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).

⁷ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. *Big Brother Watch and Others v.*

the United Kingdom [GC], Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).

⁸ The Constitution of India, arts. 14, 19 and 21. The Telecommunications Act, 2023 (Act 44 of 2023), s. 20(2).

rather than observations of surveillance operations or measurements of legal compliance.

5.1 Units of analysis and measurement

The unit is a selected legal authority, not a person, surveillance order or jurisdiction. Engagement means that a safeguard is reported as a principle, requirement or remedial concern; it does not establish that the safeguard was implemented or satisfied. A reproducible coding schedule should identify the case, pinpoint paragraph, safeguard, decision rule and legal context. The distinction between express engagement, inferred engagement and absence of discussion should be retained.

5.2 Descriptive calculations and evidential limits

For safeguard j , engagement share $p(j) = 100 \times n(j)/12$ and non-engagement count $g(j) = 12 - n(j)$. Total reported engagements equal 78 across 96 possible authority–safeguard cells, yielding a cell engagement rate of 81.25%. This is a summary of doctrinal coverage, not a score of privacy protection. The eight safeguard columns are conceptually related and must not be treated as 96 independent observations.

The aggregate table does not supply the authority-by-safeguard binary matrix or pinpoint coding evidence. Consequently, the counts are retained as reported, with arithmetic verified, but their substantive coding cannot be independently reconstructed. Jurisdiction-specific engagement rates, co-occurrence, correlations, case-level variability and coder agreement cannot be recovered. No p -values, regression coefficients, population confidence intervals or causal conclusions are estimated from this purposive corpus.

5.3 Coding sensitivity and reproducibility

One reclassified authority changes a safeguard share by 8.33 percentage points. A two-case difference therefore represents 16.67 points. This granularity makes small rank differences sensitive to coding decisions. A future replication should use independent dual coding, publish the complete coding matrix and disagreement resolutions, and then report agreement and a chance-adjusted

reliability statistic. No inter-coder reliability value is claimed here.

6. India: Constitutional And Statutory Surveillance Architecture

6.1 PUCL and the Proceduralisation of Interception

In *People's Union for Civil Liberties (PUCL) v. Union of India*, the Supreme Court described telephone tapping as a serious invasion of privacy and responded to the risk of abuse by prescribing procedural controls for interception under the then Telegraph Act framework. The decision is significant because it treats secrecy as a reason for stronger procedure: the surveillance subject generally cannot challenge an interception while it is occurring, so legality depends heavily on authorization, record keeping, time limits and review. The later statutory and rule-based frameworks retain this procedural logic, although the institutional model remains primarily executive rather than judicial.⁹

6.2 Puttaswamy: Privacy, Legality and Proportionality

Justice K.S. Puttaswamy (Retd.) v. Union of India constitutionalised privacy as an intrinsic element of liberty, dignity and autonomy. The judgments reject the proposition that privacy disappears merely because information is shared with institutions or because governance requires data. State interference requires a legal basis, a legitimate State aim and proportionality; the jurisprudence also requires procedural guarantees sufficient to protect against abuse. For surveillance law, Puttaswamy functions as the constitutional benchmark against which statutory powers must be tested.¹⁰

The Aadhaar decision applied proportionality to a large-scale identity infrastructure and demonstrates that digital governance cases require attention to data architecture, purpose, authentication, retention and private-sector access. Although Aadhaar is not an interception case, it is central to administrative surveillance analysis because it shows that data collection can be constitutional only when purpose and safeguards are sufficiently bounded.¹¹

⁹ *Union for Civil Liberties (PUCL) v. Union of India* (1997) 1 SCC 301 (judgment dated Dec. 18, 1996).

¹⁰ *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.

¹¹ (2019) 1 SCC 1 (judgment dated Sept. 26, 2018).

6.3 Telecommunications Act, 2023 and the 2024 Lawful-Interception Rules

Section 20(2) of the Telecommunications Act, 2023 permits interception, detention, disclosure or suspension of telecommunications upon the occurrence of a public emergency or in the interest of public safety, where the competent government or authorized officer considers the measure necessary or expedient for specified grounds including sovereignty and integrity, defence and security of the State, friendly relations with foreign States, public order or prevention of incitement to an offence. Reasons must be recorded in writing and the action is subject to prescribed procedure and safeguards.¹²

The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 came into force on 6 December 2024 and superseded rules 419 and 419A of the Indian Telegraph Rules for new orders. The rules designate the Union Home Secretary or the State Home Department Secretary as the competent authority, provide controlled emergency alternatives, require confirmation of certain emergency orders, create nodal-officer procedures, require review-committee scrutiny, and limit an interception order to sixty days at a time subject to renewal with an overall ceiling of 180 days. They also regulate secure records and destruction. The architecture improves procedural specificity, but authorization remains predominantly executive rather than based on a general rule of prior judicial approval.¹³

6.4 Information Technology Act, 2000: Computer-Resource Interception

Section 69 of the Information Technology Act, 2000 separately authorizes the Central or State Government, or specially authorized officers, to direct interception, monitoring or decryption of information through a computer resource on enumerated grounds such as sovereignty, security

of the State, public order and investigation of offences, subject to procedure and safeguards. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 provide the operational framework. The coexistence of telecommunications and computer-resource interception regimes demonstrates why a platform-neutral constitutional baseline is necessary: similar privacy intrusions may otherwise be governed by different statutory pathways.¹⁴

6.5 Digital Personal Data Protection Act, 2023 and Rules, 2025

The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 establish a general framework for digital personal-data processing, rights, security obligations and institutional enforcement. The 2025 Rules were notified on 13 November 2025 as part of a staged implementation process. For State surveillance, the most important analytical point is that data-protection law is not itself a comprehensive interception code. Section 17 contains exemptions, including the possibility of exempting notified State instrumentalities for specified sovereignty, security, foreign-relations and public-order purposes. The constitutional legality of surveillance therefore continues to depend on Puttaswamy and the specific law authorizing State access, not solely on ordinary data-fiduciary compliance.¹⁵

6.6 Pegasus and the Problem of Covert Device Compromise

The Pegasus litigation illustrates the limits of frameworks built around conventional network interception. Spyware capable of compromising a device may reveal communications, location, files, microphones and other information at source. In *Manohar Lal Sharma v. Union of India*, the Supreme Court constituted an independent expert process and emphasized that national-security assertions do not place State action beyond

¹² The Telecommunications Act, 2023 (Act 44 of 2023), s. 20(2).

¹³ The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, G.S.R. 754(E), Gazette of India, Extraordinary, Part II, sec. 3(i), Dec. 6, 2024, rr. 2–6.

¹⁴ The Information Technology Act, 2000 (Act 21 of 2000), s. 69; the Information Technology (Procedure

and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E), Oct. 27, 2009.

¹⁵ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 17; the Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, sec. 3(i), Nov. 13, 2025, r. 1(2).

constitutional review. The case is important even without a final merits determination because it highlights a central governance problem: technical

capability can bypass the assumptions on which conventional interception statutes were designed.¹⁶

Table 2. Contemporary Indian surveillance-related legal architecture

Legal source	Primary scope	Authorization / trigger	Key safeguards	Principal structural issue
Constitution + Puttaswamy ¹⁷	All State intrusions into privacy	Law + legitimate aim + proportionality	Judicial review; proportionality; safeguards against abuse	Constitutional test must be translated into operational controls
Telecommunications Act, 2023, s.20 + 2024 Rules ¹⁸	Messages carried by telecommunication services/networks	Public emergency/public safety plus specified statutory grounds; written reasons	Competent authority; review committee; time limits; nodal officers; record/destruction duties	General authorization is executive, not routinely judicial
Information Technology Act, 2000, s.69 + 2009 Rules ¹⁹	Information through computer resources	Enumerated national-security/public-order/investigation grounds	Written order; designated authorities; procedural safeguards; review	Overlap with telecom regime; broad digital scope
DPDP Act, 2023 + Rules, 2025 ²⁰	Processing of digital personal data	Consent/legitimate uses subject to statutory structure; State exemptions in s.17	Security and governance duties where applicable; Data Protection Board framework	Not a substitute for surveillance authorization law; exemptions matter
Pegasus proceedings ²¹	Covert device compromise / spyware allegations	Constitutional review of alleged State surveillance	Independent expert process; judicial supervision	Technology may bypass ordinary interception architecture

¹⁶ *Manohar Lal Sharma v. Union of India*, W.P. (CrI.) No. 314 of 2021, order dated Oct. 27, 2021 (Supreme Court of India).

¹⁷ The Constitution of India, arts. 14, 19 and 21. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

¹⁸ The Telecommunications Act, 2023 (Act 44 of 2023), s. 20(2). The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, G.S.R. 754(E), Gazette of India, Extraordinary, Part II, sec. 3(i), Dec. 6, 2024, rr. 2–6.

¹⁹ The Information Technology Act, 2000 (Act 21 of 2000), s. 69; the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E), Oct. 27, 2009.

²⁰ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 17; the Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, sec. 3(i), Nov. 13, 2025, r. 1(2).

²¹ *Manohar Lal Sharma v. Union of India*, W.P. (CrI.) No. 314 of 2021, order dated Oct. 27, 2021 (Supreme Court of India).

. United States: From Reasonable Expectation To Data-Intensive Search

7.1 Katz and the Shift Beyond Property

Katz v. United States moved Fourth Amendment analysis beyond physical trespass and established the familiar reasonable-expectation-of-privacy approach. The enduring importance of Katz is institutional: when digital surveillance reveals private activity without physical entry, constitutional analysis cannot be confined to property boundaries.

7.2 Riley and the Qualitative Difference of Digital Devices

Riley v. California held that police generally must obtain a warrant before searching the digital contents of a cell phone seized incident to arrest. The Court treated the quantity and quality of digital information as constitutionally significant. A smartphone is not simply another container; it can expose a dense record of communications, photographs, movements and personal associations. That logic is directly relevant to contemporary administrative surveillance using device-linked data.

7.3 Carpenter and Historical Location Data

Carpenter v. United States held that Government acquisition of historical cell-site location information was a Fourth Amendment search and that a warrant supported by probable cause was generally required. The decision limited the traditional third-party doctrine in a context where the data created a detailed chronicle of physical movements. Carpenter expressly declined to resolve foreign-intelligence and national-security collection, but its reasoning establishes that automated generation and third-party possession do not automatically eliminate privacy expectations.

7.4 Chatrie (2026) and Geofence Location History

Chatrie v. United States is the most recent major development in this comparative corpus. The Supreme Court held that police conducted a Fourth

Amendment search when they acquired Chatrie's Google Location History through a geofence process because a person has a legitimate expectation of privacy in cell-phone location data. The Court vacated and remanded so that the lower court could determine whether each stage of the warrant satisfied probable-cause and particularity requirements. Chatrie is technically important because geofence warrants begin with an area and time rather than a known suspect; the constitutional problem is therefore not merely whether a warrant exists, but whether the warrant sufficiently constrains the population and the successive narrowing process.²²

8. European Human-Rights Standards: End-To-End Safeguards

8.1 Article 8 and "Quality of Law"

Article 8 of the European Convention on Human Rights protects private life and correspondence while permitting interferences that are in accordance with law and necessary in a democratic society for specified legitimate aims. In secret-surveillance cases, the European Court of Human Rights places special weight on foreseeability and safeguards against arbitrary power because the person affected may never know that surveillance occurred.

8.2 Roman Zakharov and Szabó and Vissy

In Roman Zakharov v. Russia, the Grand Chamber found a violation of Article 8 arising from a system of secret interception that did not provide adequate safeguards against arbitrariness and abuse. Szabó and Vissy v. Hungary similarly emphasized the need for strict necessity and meaningful authorization and supervision in national-security surveillance. Together, these decisions show that a formally enacted power is insufficient if operational discretion is too broad or review is ineffective.²³

8.3 Big Brother Watch and Centrum för rättvisa

The Grand Chamber's 2021 judgments in Big Brother Watch v. United Kingdom and Centrum för rättvisa v. Sweden adapted Article 8 doctrine to bulk interception. Big Brother Watch emphasized

²² Chatrie v. United States 609 U.S. ____ (2026), No. 25-112, slip opinion (June 29, 2026), available at: https://www.supremecourt.gov/opinions/25pdf/25-112_0am4.pdf (last visited on Sept. 30, 2026).

²³ *Roman Zakharov v. Russia [GC]*, Application No. 47143/06, judgment dated Dec. 4, 2015 (European Court of Human Rights).

end-to-end safeguards, including independent authorization and controls over selectors and examination. Centrum found that deficiencies in destruction rules, protection when sharing intelligence with foreign partners and effective ex post review prevented the Swedish system from providing sufficient safeguards. The cases do not establish that bulk interception is inherently incompatible with Article 8; rather, they make the safeguards proportionate to the scale and opacity of the system.²⁴

8.4 EU Law-Enforcement Data Protection

The European Union's Law Enforcement Directive (Directive (EU) 2016/680) reinforces principles of lawfulness, purpose limitation, accuracy, security and data minimization for processing by competent authorities. Recent Court of Justice case law has continued to treat data minimization as an expression of proportionality and has emphasized the importance of prior judicial or independent administrative review for intrusive access to digital-device data. The European model therefore links surveillance authorization with downstream data-governance obligations.

10. Structured Comparative Doctrinal Analysis

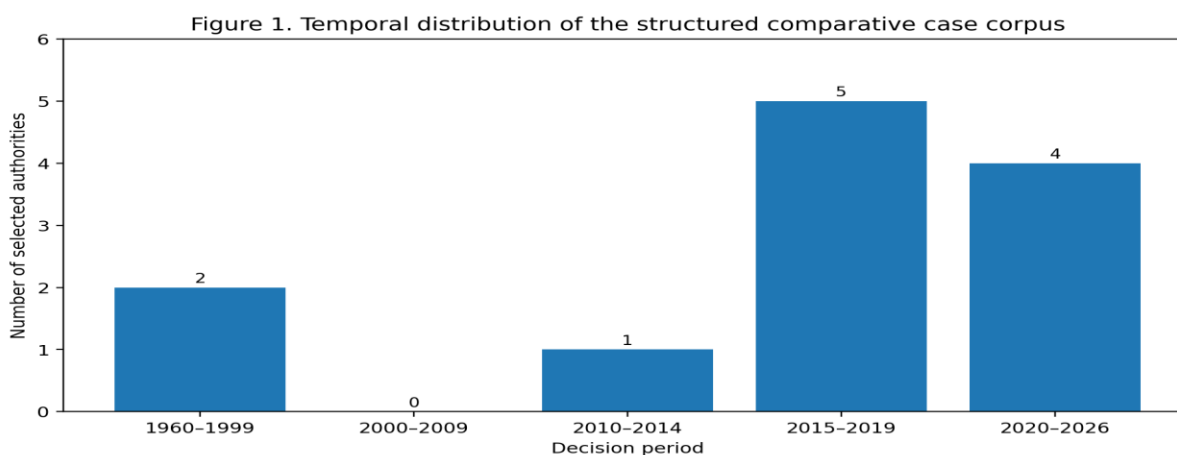


Figure 1. Temporal Distribution of the Structured Comparative Case Corpus

9. International Human-Rights Framework

Article 17 of the International Covenant on Civil and Political Rights prohibits arbitrary or unlawful interference with privacy, family, home or correspondence. The Human Rights Committee's General Comment No. 16 requires that even lawful interference not be arbitrary and that legislation specify the circumstances in which interference may occur. In the digital environment, the concept of arbitrariness necessarily incorporates reasonableness, necessity and proportionality.²⁵

The Office of the United Nations High Commissioner for Human Rights, in its 2022 report on the right to privacy in the digital age, emphasizes that contemporary data-intensive technologies can create surveillance capabilities exceeding traditional legal assumptions. International guidance increasingly converges around clear law, strict necessity, proportionality, independent oversight, limits on retention and sharing, transparency where compatible with legitimate objectives, and effective remedies.²⁶

²⁴ *Big Brother Watch and Others v. the United Kingdom [GC]*, Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).

²⁵ International Covenant on Civil and Political Rights, 1966, art. 17; United Nations Human Rights

Committee, General Comment No. 16: Article 17 (Right to Privacy), Apr. 8, 1988, paras 3–4 and 8.

²⁶ United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/51/17 (Aug. 4, 2022).

Nine of the twelve selected authorities (75.0%) date from 2015 onward. This describes the composition of the purposive corpus; it does not establish an

increase in surveillance litigation or doctrinal density over time because inclusion was not based on a comprehensive longitudinal search.

Table 3. Purposive corpus of selected surveillance and privacy authorities (N = 12)

Year	Jurisdiction	Authority	Primary surveillance/privacy context
1967 ²⁷	United States	Katz v. United States	Electronic listening / reasonable expectation of privacy
1996	India	PUCL v. Union of India	Telephone interception
2014 ²⁸	United States	Riley v. California	Search of smartphone contents
2015 ²⁹	ECtHR	Roman Zakharov v. Russia	Secret mobile-communications interception
2016 ³⁰	ECtHR	Szabó and Vissy v. Hungary	National-security secret surveillance
2017	India	Justice K.S. Puttaswamy v. Union of India	Constitutional informational privacy
2018	United States	Carpenter v. United States	Historical cell-site location information
2018	India	K.S. Puttaswamy (Aadhaar-5J.) v. Union of India	Biometric identity / authentication infrastructure
2021 ³¹	ECtHR	Big Brother Watch v. United Kingdom	Bulk interception and intelligence sharing
2021 ³²	ECtHR	Centrum för rättvisa v. Sweden	Bulk signals intelligence
2021 ³³	India	Manohar Lal Sharma v. Union of India (Pegasus)	Alleged spyware / covert device compromise
2026	United States	Chatrue v. United States	Geofence / Google Location History

Table 4. Safeguard prevalence in the coded authority corpus

Safeguard	Authorities (N)	Share	Coding meaning
Legality	12	100.0%	Expressly engaged as principle, requirement or remedial concern

²⁷ Katz v. United States 389 U.S. 347 (1967).

²⁸ 573 U.S. 373 (2014).

²⁹ *Roman Zakharov v. Russia [GC]*, Application No. 47143/06, judgment dated Dec. 4, 2015 (European Court of Human Rights).

³⁰ *Szabó and Vissy v. Hungary*, Application No. 37138/14, judgment dated Jan. 12, 2016 (European Court of Human Rights).

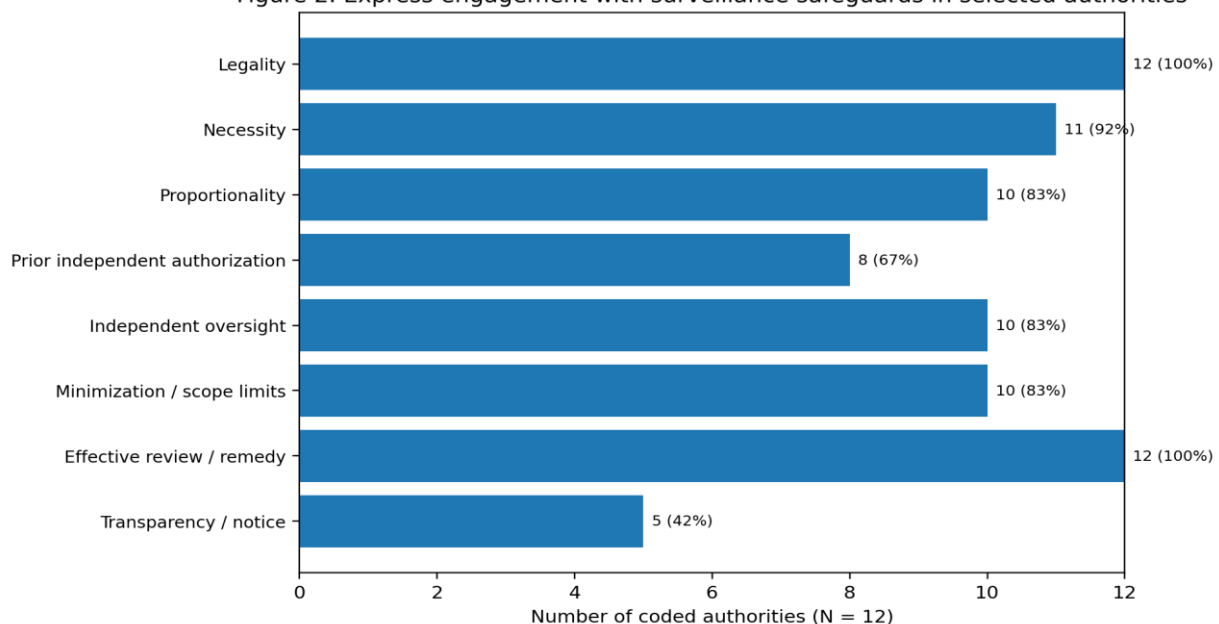
³¹ *Big Brother Watch and Others v. the United Kingdom [GC]*, Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).

³² *Centrum för rättvisa v. Sweden [GC]*, Application No. 35252/08, judgment dated May 25, 2021 (European Court of Human Rights).

³³ *Manohar Lal Sharma v. Union of India*, W.P. (CrI.) No. 314 of 2021, order dated Oct. 27, 2021 (Supreme Court of India).

Necessity	11	91.7%	Expressly engaged as principle, requirement or remedial concern
Proportionality	10	83.3%	Expressly engaged as principle, requirement or remedial concern
Prior independent authorization	8	66.7%	Expressly engaged as principle, requirement or remedial concern
Independent oversight	10	83.3%	Expressly engaged as principle, requirement or remedial concern
Minimization / scope limits	10	83.3%	Expressly engaged as principle, requirement or remedial concern
Effective review / remedy	12	100.0%	Expressly engaged as principle, requirement or remedial concern
Transparency / notice	5	41.7%	Expressly engaged as principle, requirement or remedial concern

Figure 2. Express engagement with surveillance safeguards in selected authorities

**Figure 2. Express Engagement with Surveillance Safeguards in Selected Authorities**

Three patterns are visible. First, legality and effective review or remedy are nearly universal concerns. Second, necessity and proportionality are now central across modern privacy jurisprudence even though older Fourth Amendment doctrine used different language. Third, prior independent authorization and transparency are less uniformly

developed. This divergence is institutionally important: jurisdictions may agree that surveillance must be lawful and proportionate while adopting materially different models for who authorizes it and how secrecy is later subjected to public or individual accountability.

10.1 Distribution of reported safeguard engagement

Table 5. Descriptive statistics of safeguard engagement

Statistic	Computed value	Interpretation
Total possible cells	$12 \times 8 = 96$	Authority–safeguard combinations
Reported engaged cells	78	Sum of eight safeguard counts
Reported cell engagement	81.25%	78/96; descriptive coverage
Mean across safeguard shares	81.25%	Each safeguard equally weighted
Median across safeguard shares	83.33%	Middle of eight reported shares
Minimum and maximum	41.67% and 100%	Transparency; legality and remedy
Range	58.33 percentage points	100 – 41.67
Per-authority coding increment	8.33 percentage points	100/12

Five of eight safeguards engage at least ten authorities. Legality and remedy each engage all twelve; transparency engages five, leaving seven authorities without reported engagement. Necessity exceeds prior independent authorization by 25.0 percentage points. These are within-corpus contrasts and cannot demonstrate superior institutional performance.

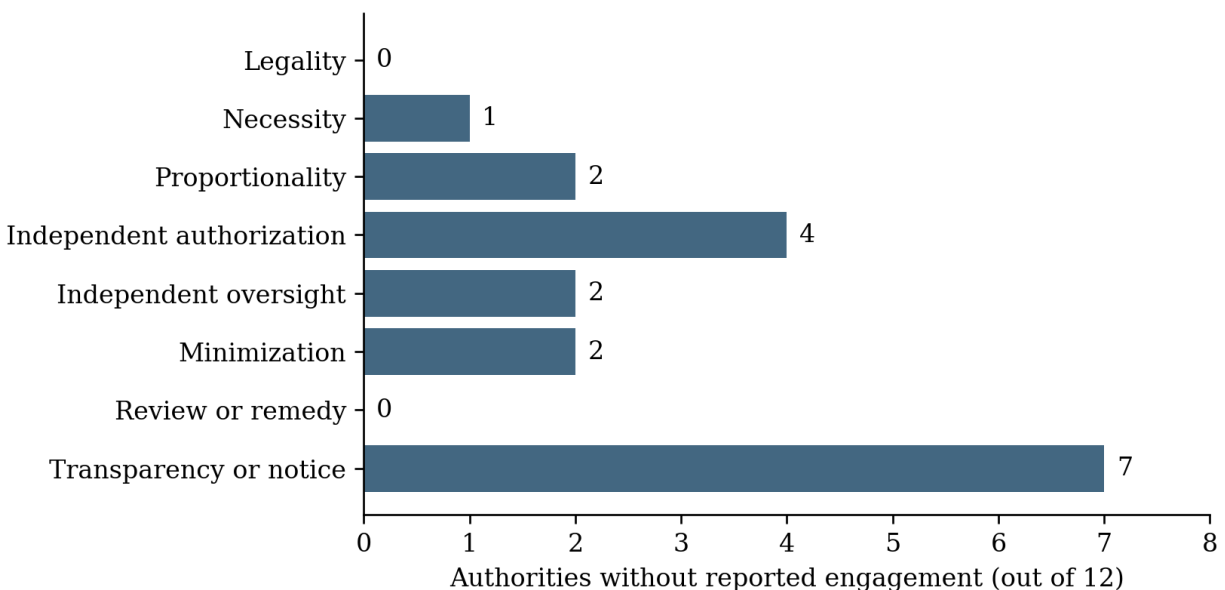


Figure 3. Complement of reported safeguard engagement in the twelve-authority corpus. Absence of reported engagement is not proof of absence of legal protection. Derived from Table 4.

10.2 Analytical grouping of safeguards

An equal-weight grouping separates core justification (legality, necessity and proportionality), institutional control (authorization, oversight and remedy), scope control (minimization) and public visibility (transparency). Their engagement rates are

91.67%, 83.33%, 83.33% and 41.67%, respectively. These groups are interpretive summaries with different numbers of indicators, not validated scales. The 50.0-point difference between justification and visibility identifies an area for closer doctrinal review.

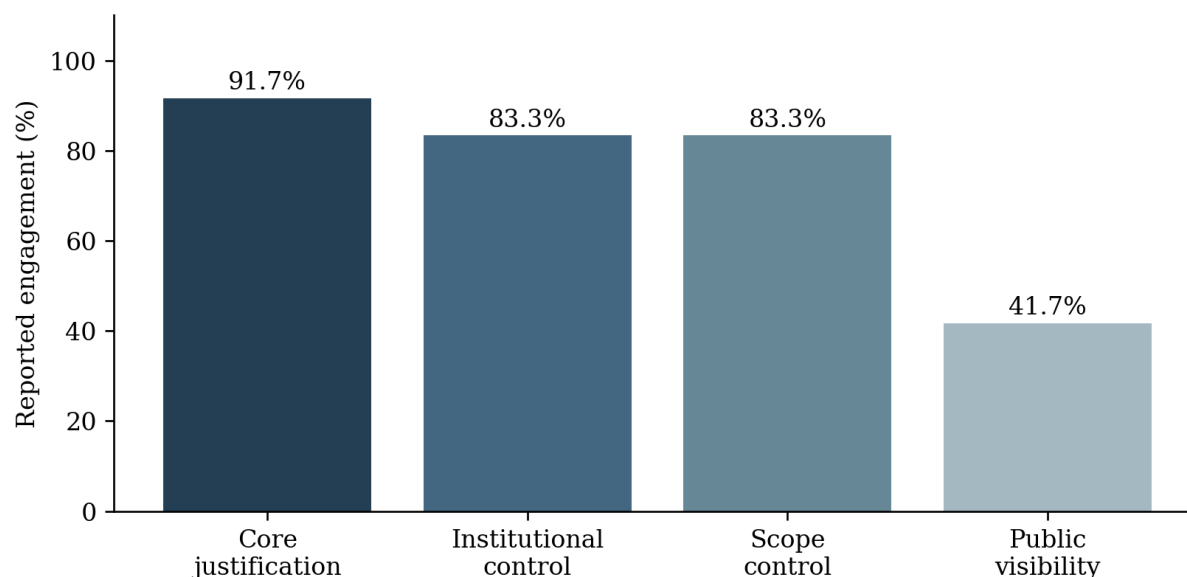


Figure 4. Engagement by analytical safeguard family. Denominators are 36, 36, 12 and 12 authority–safeguard cells, respectively. Derived from Table 4.

The corpus contains four authorities per comparative group (33.33% each), but equal representation does not make the legal systems exchangeable. The ECtHR is a supranational court;

the other groups comprise national decisions. Differences in technology, remedy, procedure and era limit any numerical ranking of jurisdictions.

Table 6. Comparative architecture of surveillance safeguards

Dimension	India	United States	ECtHR / European model
Constitutional anchor	Articles 14, 19 and 21; privacy as fundamental right	Fourth Amendment reasonableness, warrant and particularity	ECHR Article 8; EU Charter and law-enforcement data rules
Core test	Legality, legitimate aim, proportionality and procedural safeguards	Search threshold, reasonableness, warrant/probable cause subject to exceptions	In accordance with law; legitimate aim; necessity in a democratic society; proportionality
Default authorization model	Executive authorization under major interception regimes; judicial review remains available	Judicial warrant central for many criminal-investigative digital searches	Independent authorization/supervision strongly emphasized for secret or bulk regimes
Minimization logic	Time, record and destruction controls exist in specific rules; constitutional proportionality overlays them	Particularity, scope and duration constrained through warrant doctrine and case-specific limits	End-to-end safeguards, selectors, retention, sharing and destruction controls
Oversight	Executive review committees plus constitutional courts	Neutral magistrate, suppression litigation and appellate review	Independent authorization/supervision plus ex post review and ECtHR remedy

Transparency / notice	Limited by secrecy; judicial challenges and public rules provide partial transparency	Notice often through criminal process; warrant litigation creates ex post visibility	Notification may be delayed; system-level transparency and effective review are key safeguards
Primary modern challenge	Integrating constitutional proportionality with executive interception systems and emerging data infrastructures	Applying warrant doctrine to population-scale queries and third-party data	Maintaining effective end-to-end safeguards for bulk and cross-border intelligence systems

11. Technology-Specific Legal Risk Analysis

11.1 Facial Recognition and Biometric Identification

Facial recognition converts visual observation into scalable identification. The constitutional risk increases when watchlists are broad, matching thresholds are opaque, images are retained for

provide audit trails capable of reconstructing how a match was generated and acted upon.³⁴

11.2 Predictive Analytics and Algorithmic Risk Scoring

Predictive systems create a different form of surveillance because they infer future risk rather than merely recording past behaviour. The legal problem is not solved by declaring the algorithm “advisory.” If a score influences policing, border decisions, benefits, licensing or investigation priority, the State should be able to identify the lawful purpose, the data categories used, validation criteria, material error risks and the role of human decision-makers. Necessity and proportionality require attention to both model input and downstream consequence.

11.3 Location, Geofence and Mobility Data

Carpenter and Chatrre illustrate why location data deserve special treatment. Even a short observation can reveal presence in a home or another sensitive place, while longer histories reconstruct patterns of association and behaviour. Geofence methods create an additional inversion: they identify persons from a place-time query rather than searching a known person. Particularity, probabilistic

unrelated purposes, or a match triggers adverse action without human verification. A privacy-resilient framework should therefore separate image capture from identity resolution, require a defined purpose and legal basis for watchlist creation, document matching thresholds and human-review rules, restrict secondary use, and

justification, staged minimization and independent control over successive de-anonymization steps are therefore critical.

11.4 Bulk Interception, Metadata and Data Fusion

Bulk systems challenge individualised authorization because collection may precede identification of a particular person. The ECtHR response is to require safeguards at every stage: authorization of the system, definition of categories and selectors, controls on examination, retention and destruction, rules for intelligence sharing, and independent ex post review. This lifecycle model is also useful for administrative data-fusion systems, where risk may arise from querying and enrichment rather than initial collection.³⁵

11.5 Quantifying location data intrusiveness

Chatrre describes approximately 720 daily Location History chartings compared with 101 daily CSLI chartings discussed in Carpenter: a ratio of 7.13 and an increase of approximately 612.9%. The comparison illustrates temporal sampling density; it

³⁴ United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/51/17 (Aug. 4, 2022).

³⁵ *Big Brother Watch and Others v. the United Kingdom [GC]*, Application Nos. 58170/13,

62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).

does not measure all devices, current provider practices or a sevenfold increase in constitutional harm. Spatial precision, sensitivity of places,

retention and inference remain separate dimensions. Chatric, slip opinion, syllabus pp. 1–3 and opinion pp. 16–18.

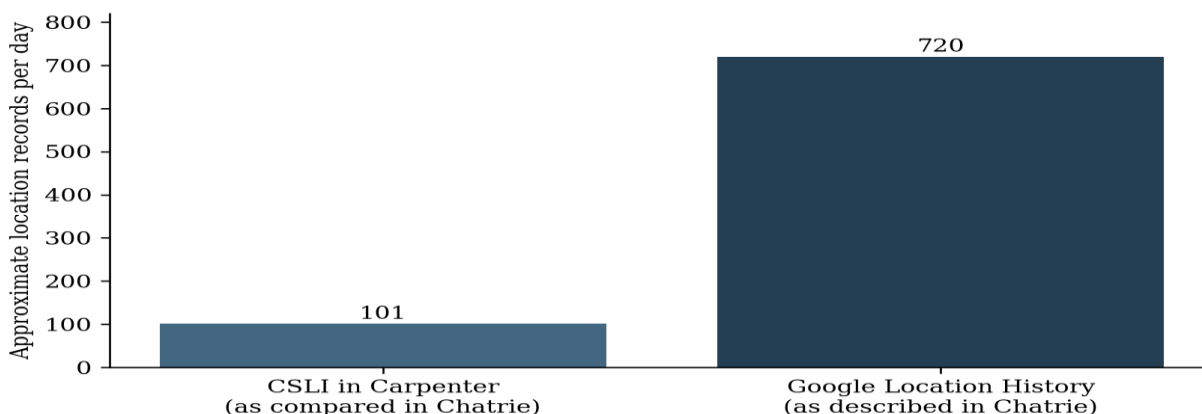


Figure 5. Approximate daily location sampling described in Chatric. Values 101 and 720 are judiciously described comparison figures, not a new experimental dataset.

The warrant described in Chatric initially used a 150-metre radius and a one-hour window, followed by a two-hour expanded data stage and subsequent identification. A circular 150-metre region has an area of approximately 70,686 m² (0.0707 km²). Under a simplified uniform-density assumption, halving radius to 75 metres reduces area by 75%, while halving time reduces space–time exposure by 50%; applying both reduces it by 87.5%. These are geometric sensitivities, not measured reductions in affected persons. Location uncertainty, uneven occupancy and query expansion must be assessed separately.

11.6 Base rates and false positive burden

For a binary alerting system, sensitivity = $TP / (TP + FN)$, false positive rate = $FP / (FP + TN)$, and positive predictive value (PPV) = $TP / (TP + FP)$. For target prevalence π , sensitivity s and false positive rate f , $PPV = s\pi / [s\pi + f(1 - \pi)]$. A low false positive rate can still produce many erroneous alerts when screening a large population with rare targets. In one-to-many facial identification, pairwise false match rates and search-level false positive identification rates must be distinguished. NISTIR 8280 documents demographic effects and the dependence of interpretation on evaluation conditions.

Table 7. Illustrative expected alert outcomes

Assumed FPR	Expected true alerts	Expected false alerts	PPV
0.01%	95	9.99	90.49%
0.10%	95	99.9	48.74%
1.00%	95	999	8.68%

Illustrative assumptions for this table are 100,000 independent binary screening decisions, target prevalence 0.1% (100 true targets), sensitivity 95% and fixed operating thresholds. Counts are expectations, hence may be fractional. They are not measured facial recognition or policing outcomes. At 0.10% FPR, almost half of alerts are false despite 95% sensitivity. Human review must be evaluated independently; it cannot be assumed to remove all error.

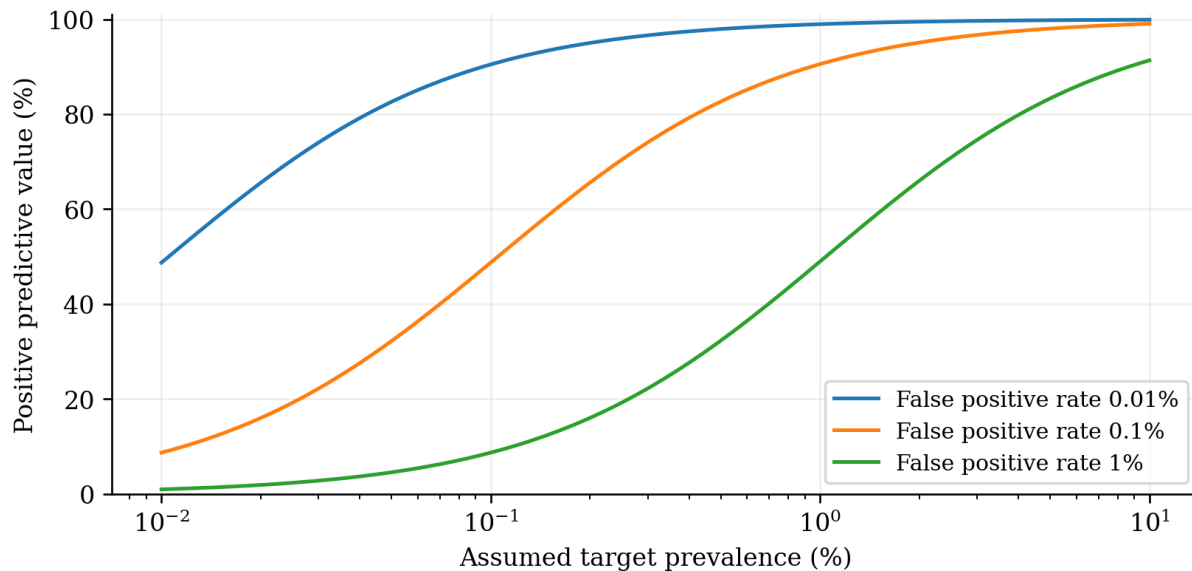


Figure 6. Illustrative PPV sensitivity to prevalence and false positive rate, holding sensitivity at 95%. Mathematical scenario only; not empirical surveillance data.

11.7 Retention and cumulative data exposure

At a constant acquisition rate λ and retention period T , retained volume $V = \lambda T$ in steady state, assuming no duplicates, selective preservation or backlog. At an illustrative λ of 10,000 records per day, retention of 7, 30, 60, 90 and 180 days yields

70,000, 300,000, 600,000, 900,000 and 1,800,000 records. Extending retention from 30 to 180 days multiplies volume by six; shortening 180 days to 30 reduces it by 83.33%. These are engineering scenarios, not legal retention limits or actual operating volumes.

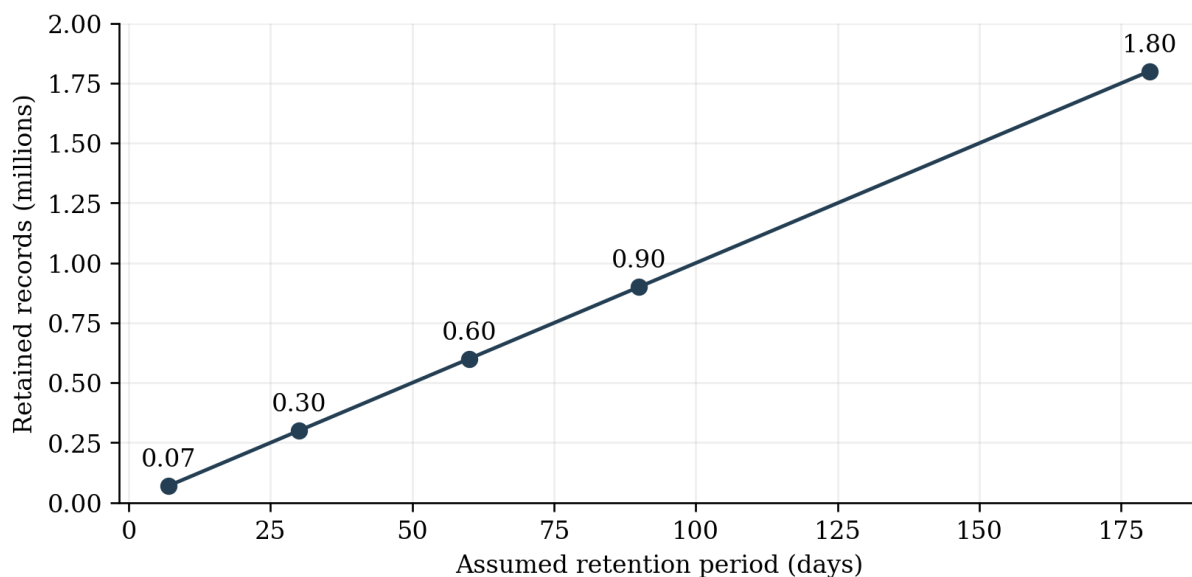


Figure 7. Illustrative retained volume at 10,000 records per day. Linear model assumes constant acquisition and complete deletion at expiry.

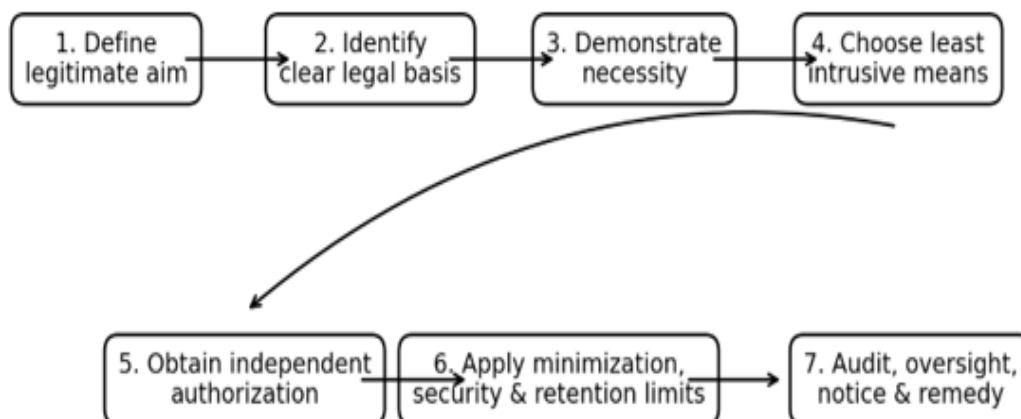
Retained volume measures inventory rather than privacy harm. Replicas, backups, derived embeddings, identity links and shared copies can preserve exposure after source deletion. Retention controls should therefore cover

source and derived data, record deletion completion, and distinguish ordinary expiry from separately justified legal preservation.

Table 8. Technology-to-safeguard mapping for modern administrative surveillance

Technology	Trigger requiring enhanced scrutiny	Required safeguards
Facial recognition	Identification at scale or use of sensitive watchlists	Statutory purpose; watchlist governance; accuracy testing; human verification; audit logs; retention limits
Biometric databases	Persistent identifiers linked across services	Purpose separation; access segmentation; encryption; breach controls; deletion rules; independent audit
Geofence / location history	Area-time search capable of identifying unknown individuals	Probable cause or equivalent strict necessity; geographic/time particularity; staged minimization; independent authorization
Predictive analytics	Risk score influences coercive or rights-affecting action	Validated model; documented features; bias/error review; human decision responsibility; contestability
Bulk interception	Population-scale collection or selector-based intelligence	Independent authorization; end-to-end safeguards; selector controls; retention/destruction; sharing rules; ex post review
Cross-database data fusion	Combining datasets collected for different original purposes	Legal basis for linkage; purpose compatibility; query approval; role-based access; immutable audit trail; periodic necessity review

12. A RIGHTS-BASED SURVEILLANCE GOVERNANCE MODEL



Failure at legality, legitimate aim or necessity should terminate authorization; later stages govern scope and accountability.

Figure 8. Constitutional safeguards across the surveillance lifecycle.

The proposed model converts constitutional proportionality into a sequence of auditable

decisions. It is designed to be technology-neutral: the same gates apply whether the State seeks

communications, location data, biometric matching, predictive output or fused administrative records. However, the intensity of the safeguards should increase with scale, sensitivity, secrecy and automation.

12.1 Gate 1: Clear Legal Basis and Defined Purpose

Every surveillance operation should identify the precise statutory provision and the specific legitimate aim relied upon. Broad references to security or public interest should not substitute for a recorded link between the legal ground and the operational objective. The authorizing record should identify the person, class, selector, dataset, place, time period or threat category with the greatest specificity compatible with the technique.

12.2 Gate 2: Demonstrated Necessity and Less-Intrusive Alternatives

The authority should document why the information is needed and why materially less

12.4 Gate 4: Independent Authorization and Oversight

The comparative jurisprudence demonstrates the value of independent authorization, especially for intrusive or secret surveillance. India's current major interception regimes rely principally on senior executive authorization combined with review committees. A stronger architecture for highly intrusive digital surveillance would separate the operational requester from the approving authority and require a body institutionally capable of testing necessity and proportionality rather than merely verifying formal compliance.³⁶

12.6 Measurable controls for implementation

intrusive methods are inadequate. Necessity is particularly important for biometric, bulk or geofence techniques because their capacity to implicate non-targets is structurally high. The analysis should address the expected evidentiary or administrative value, alternatives attempted, and the consequence of non-collection.

12.3 Gate 3: Proportionality and Scope Engineering

Proportionality should be implemented through system parameters: query radius, time window, selectors, confidence thresholds, data categories, access permissions, de-anonymization stages, retention periods and onward sharing. A legally proportionate system is therefore one whose technical settings are traceable to the justification accepted at authorization.

12.5 Gate 5: Accountability, Transparency and Remedy

Secrecy may be operationally necessary during surveillance, but perpetual opacity is not. Systems should generate immutable authorization and access logs, periodic statistical transparency where security permits, independent audits, and delayed notice where notice no longer creates a serious risk. Effective remedies should include cessation, deletion, correction of downstream records, exclusion or non-use where appropriate, and compensation or other judicial relief when unlawful surveillance causes harm.

Table 9. Proposed implementation metrics

Control	Operational measure	Validation requirement
Scope minimization	Released records / initially retrieved records	Record stage-specific denominators and reasons for release
Authorization traceability	Queries with valid authorization / all queries	Validate scope and expiry, not only existence of an ID
Retention compliance	Expired records deleted / records due for deletion	Include derived data and audit deletion lag

³⁶ *Big Brother Watch and Others v. the United Kingdom [GC]*, Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25,

2021, paras 350–359 (European Court of Human Rights).

Alert quality	PPV, sensitivity and FPR	Use labelled deployment-relevant validation data
Group error disparity	Group FPR and FNR; absolute rate differences	Report sample sizes and uncertainty; examine image quality
Audit completeness	Logged sensitive operations / all sensitive operations	Test logging coverage, tamper evidence and access separation
Remedial effectiveness	Time to correction or deletion after upheld complaint	Track downstream copies and recurring violations

These are proposed monitoring measures, not observed study results. Thresholds must be justified for the technology, deployment conditions and rights impact. Cryptographic log chaining, digitally signed approvals, role separation, encryption and least-privilege access support auditability, but do not themselves establish necessity or constitutional proportionality. A valid approval should bind purpose, selectors, data fields, spatial extent, duration, model version and permitted recipients.

12.7 Limits of the quantitative interpretation

The statistical component is a descriptive augmentation of doctrinal analysis. The sample is small and purposive, engagement is not equivalent to enforcement, and aggregate counts conceal differences between judicial recognition, remedial concern and operational practice. The numerical simulations show parameter sensitivity without validating any deployed surveillance system. Testing compliance or effectiveness would require operational records, representative error datasets, published coding evidence and separately designed empirical research.

13. Principal Findings

- The comparative legal systems increasingly converge on legality, necessity, proportionality and effective review as the core grammar of surveillance control.³⁷

- Prior independent authorization is more structurally embedded in United States criminal-search doctrine and ECtHR secret-surveillance standards than in India's principal statutory interception model, which continues to rely primarily on executive authorization and review committees.
- India's 2024 telecommunications interception rules improve procedural specificity through competent-authority rules, confirmation requirements, review mechanisms, time limits and destruction controls, but they do not eliminate the need for constitutional proportionality review under Puttaswamy.
- The DPDP framework strengthens general digital-data governance but does not operate as a complete surveillance authorization code; statutory exemptions and separate interception powers remain legally significant.³⁸
- Carpenter and Chatrue demonstrate that third-party possession and automated generation of location data do not automatically extinguish constitutional privacy, and that the scope and particularity of data requests matter independently of the mere existence of a warrant.³⁹
- The ECtHR's "end-to-end safeguards" approach is particularly suitable for AI, bulk interception and data-fusion systems because privacy risk may intensify during filtering, analysis, sharing and retention after initial acquisition.⁴⁰

³⁷ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. *Carpenter v. United States*, 585 U.S. 296 (2018).

³⁸ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 17; the Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, sec. 3(i), Nov. 13, 2025, r. 1(2).

³⁹ 585 U.S. 296 (2018). 609 U.S. ____ (2026), No. 25-112, slip opinion (June 29, 2026), available at: https://www.supremecourt.gov/opinions/25pdf/25-112_0am4.pdf

⁴⁰ *Big Brother Watch and Others v. the United Kingdom [GC]*, Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).

- Transparency remains the least consistently developed safeguard in the coded corpus. Secret surveillance requires alternative accountability mechanisms such as independent review, auditability, delayed notice and public reporting at an aggregate level. Its 41.67% reported engagement share is 58.33 percentage points below legality and remedy; this describes doctrinal visibility in the selected corpus rather than the frequency of unlawful surveillance.
- A technology-neutral statute is insufficient unless technical parameters—selectors, retention, access rights, thresholds and de-anonymization stages—are aligned with the legal necessity and proportionality finding.

14. Recommendations

- Adopt a consolidated, platform-neutral surveillance safeguards statute or code that applies minimum constitutional standards across
- Establish immutable audit logs and periodic independent audits capable of reconstructing who queried what data, under which authorization, for what purpose and with what downstream action.
- Introduce clearer retention and destruction schedules, with preservation beyond default limits requiring renewed justification and authorization.
- Create aggregate transparency reporting for surveillance orders and technology classes, while allowing narrowly tailored redactions for operational security.
- Provide delayed notification to affected individuals when secrecy is no longer necessary, subject to judicially reviewable exceptions, so that rights and remedies are not purely theoretical.
- Ensure that evidence or administrative decisions materially derived from unlawful surveillance are subject to meaningful judicial consequences, including non-use, correction, deletion or other appropriate relief.

15. Conclusion

The central challenge of contemporary surveillance law is no longer simply to decide whether the State may intercept a particular communication. Administrative surveillance increasingly operates through interconnected infrastructures capable of persistent observation, automated identification

telecommunications, computer resources, device compromise, location data, biometrics and administrative data fusion.

- Require prior judicial or functionally independent authorization for highly intrusive surveillance, subject to narrowly defined emergency procedures and prompt independent confirmation.
 - Make necessity documentation mandatory: the requesting authority should identify the specific objective, alternatives considered, anticipated data categories, non-target impact and expected duration.
 - Embed proportionality into technical configuration by limiting selectors, geography, duration, dataset fields, confidence thresholds, access roles, retention and onward sharing.
 - Require technology-specific impact assessments for facial recognition, biometric identification, predictive analytics, geofence searches and large-scale data matching before deployment.
- and inferential analysis. The constitutional danger lies in the combination of scale, secrecy, data linkage and automation. A legal rule that was adequate for a discrete telephone interception may be inadequate when the same State objective is pursued through geofence queries, biometric watchlists, predictive scoring or cross-database analytics.

The comparative analysis demonstrates substantial normative convergence. Indian constitutional privacy doctrine, United States digital-search jurisprudence and European human-rights law all resist the idea that technological convenience can itself justify intrusion. The strongest common principles are legality, necessity, proportionality and effective review. The major institutional divergence concerns authorization and transparency. The United States commonly relies on prior judicial warrants for criminal investigative searches; the ECtHR demands independent safeguards particularly for secret and bulk regimes; India's principal statutory interception system continues to centre senior executive authorization supplemented by review committees and constitutional judicial review.⁴¹

The future resilience of privacy therefore depends on converting constitutional principles into surveillance-system architecture. A rights-based

⁴¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC

model should require a defined legal basis and legitimate aim, demonstrated necessity, the least intrusive reasonably effective method, independent authorization for high-risk surveillance, minimization of collection and use, controlled retention, auditable access, independent oversight and meaningful remedy. These controls need not disable legitimate security or administrative functions. Properly designed, they increase the reliability and legitimacy of State action by ensuring

that surveillance remains exceptional, reasoned, bounded and reviewable.

Privacy in the digital age should not be understood as a barrier to governance. It is a constitutional discipline on how governance uses informational power. The appropriate balance is therefore not achieved by choosing privacy over security or security over privacy, but by designing surveillance institutions in which technological capability is matched by equally capable legal restraint.

References

- Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1. (1997) 1 SCC 301 (judgment dated Dec. 18, 1996). The Telecommunications Act, 2023 (Act 44 of 2023), s. 20(2).
- Carpenter v. United States, 585 U.S. 296 (2018). 609 U.S. (2026), No. 25-112, slip opinion (June 29, 2026), available at: https://www.supremecourt.gov/opinions/25pdf/25-112_0am4.pdf (last visited on Sept. 30, 2026).
- Daniel J. Solove, "A Taxonomy of Privacy" 154 *University of Pennsylvania Law Review* 477 (2006). Neil M. Richards, "The Dangers of Surveillance" 126 *Harvard Law Review* 1934 (2013).
- United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/51/17 (Aug. 4, 2022).
- The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 17; the Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, sec. 3(i), Nov. 13, 2025, r. 1(2).
- Big Brother Watch and Others v. the United Kingdom [GC]*, Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).
- Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. *Big Brother Watch and Others v. the United Kingdom [GC]*, Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).
- The Constitution of India, arts. 14, 19 and 21. The Telecommunications Act, 2023 (Act 44 of 2023), s. 20(2).
- Union for Civil Liberties (PUCI) v. Union of India (1997) 1 SCC 301 (judgment dated Dec. 18, 1996).
- Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.
- K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1 (judgment dated Sept. 26, 2018).
- The Telecommunications Act, 2023 (Act 44 of 2023), s. 20(2).
- The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, G.S.R. 754(E), Gazette of India, Extraordinary, Part II, sec. 3(i), Dec. 6, 2024, rr. 2–6.
- The Information Technology Act, 2000 (Act 21 of 2000), s. 69; the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E), Oct. 27, 2009.
- The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 17; the Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, sec. 3(i), Nov. 13, 2025, r. 1(2).
- Manohar Lal Sharma v. Union of India*, W.P. (Crl.) No. 314 of 2021, order dated Oct. 27, 2021 (Supreme Court of India).
- The Constitution of India, arts. 14, 19 and 21. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- The Telecommunications Act, 2023 (Act 44 of 2023), s. 20(2). The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, G.S.R. 754(E), Gazette of India, Extraordinary, Part II, sec. 3(i), Dec. 6, 2024, rr. 2–6.
- The Information Technology Act, 2000 (Act 21 of 2000), s. 69; the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E), Oct. 27, 2009.

The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 17; the Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, sec. 3(i), Nov. 13, 2025, r. 1(2).

Manohar Lal Sharma v. Union of India, W.P. (Crl.) No. 314 of 2021, order dated Oct. 27, 2021 (Supreme Court of India).

Chatrie v. United States 609 U.S. ____ (2026), No. 25-112, slip opinion (June 29, 2026), available at: https://www.supremecourt.gov/opinions/25pdf/25-112_0am4.pdf

Roman Zakharov v. Russia [GC], Application No. 47143/06, judgment dated Dec. 4, 2015 (European Court of Human Rights).

Roman Zakharov v. Russia [GC], Application No. 47143/06, judgment dated Dec. 4, 2015 (European Court of Human Rights).

Big Brother Watch and Others v. the United Kingdom [GC], Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).

International Covenant on Civil and Political Rights, 1966, art. 17; United Nations Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), Apr. 8, 1988, paras 3–4 and 8.

United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/51/17 (Aug. 4, 2022).

Katz v. United States 389 U.S. 347 (1967).

Riley v. California, 573 U.S. 373 (2014).

Roman Zakharov v. Russia [GC], Application No. 47143/06, judgment dated Dec. 4, 2015 (European Court of Human Rights).

Szabó and Vissy v. Hungary, Application No. 37138/14, judgment dated Jan. 12, 2016 (European Court of Human Rights).

Big Brother Watch and Others v. the United Kingdom [GC], Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).

Centrum för rättvisa v. Sweden [GC], Application No. 35252/08, judgment dated May 25, 2021 (European Court of Human Rights).

Manohar Lal Sharma v. Union of India, W.P. (Crl.) No. 314 of 2021, order dated Oct. 27, 2021 (Supreme Court of India).

United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/51/17 (Aug. 4, 2022).

Big Brother Watch and Others v. the United Kingdom [GC], Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).

Big Brother Watch and Others v. the United Kingdom [GC], Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. *Carpenter v. United States*, 585 U.S. 296 (2018).

The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 17; the Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, sec. 3(i), Nov. 13, 2025, r. 1(2).

Carpenter v. United States, 585 U.S. 296 (2018). 609 U.S. ____ (2026), No. 25-112, slip opinion (June 29, 2026), available at: https://www.supremecourt.gov/opinions/25pdf/25-112_0am4.pdf

Big Brother Watch and Others v. the United Kingdom [GC], Application Nos. 58170/13, 62322/14 and 24960/15, judgment dated May 25, 2021, paras 350–359 (European Court of Human Rights).

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.

Patrick Grother, Mei Ngan and Kayee Hanaoka, Face Recognition Vendor Test Part 3 Demographic Effects, NISTIR 8280 (2019), <https://doi.org/10.6028/NIST.IR.8280>.

Chatrie v. United States, No. 25-112, slip opinion (29 June 2026), syllabus pp. 1–3, opinion pp. 16–18, https://www.supremecourt.gov/opinions/25pdf/25-112_0am4.pdf.