# THE RIGHT TO PRIVACY AND MASS SURVEILLANCE: COMPARATIVE ANALYSIS POST-2020

REVA NAIDU*

*This commentary explores whether existing international and constitutional protections are adequate in the face of rapidly expanding surveillance technologies, and whether we need doctrinal and institutional reform.*



* LL.M in International Legal Studies, New York University School of Law, Senior Commentary Editor, Journal of International Law and Politics, and LL.B. (Hons), The University of Law.

## I. INTRODUCTION

The right to privacy remains one of the most vigorously defended and most rapidly eroding pillars of the international human rights framework. Explicitly codified in Article 17 of the International Covenant on Civil and Political Rights (ICCPR),[1] Article 12 of the Universal Declaration of Human Rights (UDHR),[2] and Article 8 of the European Convention on Human Rights (ECHR);[3] this right imposes a clear negative obligation on states to refrain from arbitrary interference with the private lives of individuals. However, the last decade has witnessed a dramatic, near-ubiquitous expansion of mass state-sponsored surveillance capabilities. This technological drift accelerated under exceptional circumstances, notably during the COVID-19 pandemic,[4] where public health rationales were leveraged to normalize highly invasive data collection practices, including mandatory contact tracing and location data collection.[5] This trajectory has been further solidified by the continuous deployment of powerful tools like universal facial recognition and programmatic data exploitation by government agencies.[6]

This growing reliance on surveillance technology has generated a profound constitutional dilemma for liberal democracies.[7] The core tension lies in reconciling the state's legitimate duties such as maintaining national security, public order, and public health with individual citizens' fundamental rights to privacy, autonomy, and non-interference.[8] The resulting friction between collective security imperatives and individual digital liberty is reshaping the current constitutional and jurisprudential landscape globally. This commentary, therefore, addresses whether international and domestic constitutional protections, predominantly formulated within the analog context of the 20th

---

1. International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

2. Universal Declaration of Human Rights art. 12, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948).

3. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

4. David Lyon, *Pandemic Surveillance* 3 (2022).

5. Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 Harv. Int'l L.J. 81 (2015).

6. Shoshana Zuboff, *The Age of Surveillance Capitalism* 130 (Profile Books 2019).

7. P. Königs, Government Surveillance, Privacy, and Legitimacy, 35 PHIL. TECH. 8 (2022).

8. Am. Civil Liberties Union, Privacy and Surveillance, https://www.aclu.org/issues/national-security/privacy-and-surveillance (last visited Oct. 24, 2025).

century, are doctrinally adequate to protect individual rights against the challenges posed by rapidly expanding 21st-century surveillance technologies, or if there is a compelling necessity for systemic legal and institutional reform. To conduct this analysis, this commentary will first provide a comparative survey of jurisprudential and legislative responses across the EU, the US, India, and China. It will then analyze the crisis through the lens of international human rights law, concluding with an assessment of proposed doctrinal and institutional mechanisms aimed at rectifying the contemporary privacy deficit.

## II. INTERNATIONAL LEGAL FRAMEWORK ON PRIVACY

The global protection of privacy is anchored in a variety of treaties, regional conventions, and soft law instruments, yet it faces significant challenges in enforcement and adapting to rapid technological advancement.

At the universal level, the cornerstone is the International Covenant on Civil and Political Rights (ICCPR). Its Article 17 is the primary provision, prohibiting "arbitrary or unlawful interference" with an individual's privacy, family, home, or correspondence. The UN Human Rights Committee's General Comment No. 16 clarifies this obligation,[9] detailing the scope of privacy and the limits on state interference, emphasizing legality and non-arbitrariness. Regionally, the European Convention on Human Rights (ECHR) offers the most robust protection. Article 8 guarantees the right to respect for private and family life, home, and correspondence. Crucially, the European Court of Human Rights has established strict tests for any permissible interference by the state: the interference must be provided by law, pursue a legitimate aim, and, most importantly, be "necessary in a democratic society."[10] This standard requires the state action to be both proportionate and based on pressing social needs. The Inter-American system has a developing framework for privacy, primarily articulated through the American Convention on Human Rights. While principles exist, the overall legal and enforcement framework is generally considered less elaborated and less frequently applied than its European counterpart.

---

9. U.N. Hum. Rts. Comm., General Comment No. 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Art. 17), ¶¶ 1–10, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (Apr. 8, 1988)

10. Council of Eur., *Articles 8–11: The Right to Respect for Private and Family Life, Freedom of Thought, Conscience and Religion, and Freedom of Expression* (ECHR Toolkit), https://www.coe.int/en/web/echr-toolkit/home/-/asset_publisher/fkfsaHu5YJRE/content/articles-8-11 (last visited Oct. 24, 2025).

Beyond binding treaties, soft law and expert reports shape the discourse and state obligations. Key contributors include the UN Special Rapporteur on the Right to Privacy and various UN High Commissioner reports on surveillance and human rights.[11] For example, the UN High Commissioner for Human Rights' 2018 report *The Right to Privacy in the Digital Age* is an authoritative "soft-law" report (A/HRC/39/29) articulates minimum standards for lawful surveillance. For instance, it insists that any surveillance must be based on publicly accessible law; secret rules or secret interpretations do not count as "law." The report emphasizes that surveillance legislation should clearly define the categories of individuals subject to monitoring, the scope, and duration, to avoid overbreadth. It also calls for independent authorization (preferably judicial) and continuous oversight by independent bodies (administrative, judicial, parliamentary) to supervise surveillance activities throughout their lifecycle. Similarly, in its 2022 report (A/HRC/51/17), OHCHR raises concerns about the growing misuse of intrusive hacking tools or spyware by states as well as extrajudicial access to personal devices.

The report strongly affirms encryption as a fundamental enabler of privacy: weakening encryption (or forcing backdoors) is treated as a serious risk to human rights. It also highlights the risk of pervasive monitoring in public and shared spaces, and calls for proportionate limits, specificity, and independent oversight. The report's recommendations to states include: adopt robust privacy legislation; ensure hacking is authorized only in narrowly defined circumstances; and guarantee meaningful oversight and remedies.

While these documents do not create binding obligations, they interpret and operationalize treaty provisions, offering persuasive authority that influences state behavior, judicial reasoning, and policy formulation. By articulating normative expectations and identifying best practices, soft law materials help to bridge gaps between formal legal commitments and real-world implementation, effectively setting international standards and heightening global awareness of surveillance-related human rights risks.

The primary gap in this extensive framework is two-fold: (1) Weak Enforcement Mechanisms: While the laws and norms may be clear, compliance is not uniform, and true global enforcement is difficult. (2) Technological Adaptability: The existing treaties predate the

11. See U.N. Special Rapporteur on the Right to Privacy, *Report on Artificial Intelligence and Privacy*, U.N. Doc. A/75/147 (July 27, 2020); Office of the U.N. High Comm'r for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (June 30, 2014)

digital age, resulting in difficulties in applying these protections to emerging technologies like Artificial Intelligence (AI), biometrics, and predictive policing. The legal frameworks struggle to effectively govern transnational data flows and state/corporate surveillance enabled by these new tools.[12]

## III. COMPARATIVE JURISDICTIONS

### *The European Union and the ECHR: Constitutionalizing Data Protection*

The European Union's data protection regime is anchored in the General Data Protection Regulation (GDPR), which operationalizes the rights to privacy and data protection guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR).[13] Its core principles are lawfulness, fairness, purpose limitation, and accountability, which codify the notion of informational self-determination first articulated by the German Federal Constitutional Court.[14] The GDPR's extraterritorial scope and the supervisory authority system under Article 51 establish it as a constitutionalised model of data governance.[15]

The Court of Justice of the European Union (CJEU) has reinforced these standards in landmark judgments. In Schrems I (2015), the Court invalidated the EU–US Safe Harbor decision for failing to guarantee "essentially equivalent" protection against disproportionate U.S. surveillance.[16] In Schrems II (2020),[17] the Privacy Shield framework was likewise annulled, as U.S. surveillance under FISA §702 and Executive Order 12333 was deemed incompatible with EU fundamental rights. The European Court of Human Rights (ECHR), applying Article 8 ECHR, similarly emphasised proportionality and independent oversight in *Big Brother Watch and Others v. United Kingdom*.[18] The Court

12. Ana Brian Nougrères (Special Rapporteur on the Right to Privacy), *Legal Safeguards for Personal Data Protection and Privacy in the Digital Age: Report of the Special Rapporteur on the Right to Privacy*, U.N. Doc. A/HRC/55/46, at 10 (Jan. 18 2024).

13. *Charter of Fundamental Rights of the European Union* arts. 7–8, 2012 O.J. (C 326) 391.

14. *Volkszählungsurteil* (Census Act Case), BVerfGE 65, 1 (Dec. 15, 1983) (F.R.G.).

15. *Regulation (EU) 2016/679 of the European Parliament and of the Council* arts. 51–59, 2016 O.J. (L 119) 1 (General Data Protection Regulation).

16. Case C-362/14, Maximillian Schrems v. Data Protection Comm'r (Schrems I), EU:C:2015:650.

17. Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. & Schrems (Schrems II), EU:C:2020:559.

18. *Big Brother Watch & Others v. United Kingdom*, App. No. 58170/13 (Eur. Ct. H.R. May 25, 2021).

accepted the legitimacy of bulk interception in principle but required safeguards such as prior authorisation and post-hoc review.

Despite its robustness, the EU model tolerates limited national-security derogations under Article 4(2) TEU, allowing Member States discretion in intelligence operations.[19] Scholars note that the tension between supranational rights and national security autonomy defines the EU's ongoing struggle to reconcile privacy with collective defence.[20]

*The United States: Constitutionalism Without a Comprehensive Statute*

Privacy protection in the United States derives primarily from the Fourth Amendment,[21] interpreted in *Katz v. United States* (1967) to protect people rather than places, and operationalised through the "reasonable expectation of privacy" test.[22] Yet digital surveillance has eroded these expectations. In *Carpenter v. United States* (2018), the Supreme Court held that accessing historical cell site data without a warrant violates the Fourth Amendment—an incremental adaptation to the realities of pervasive tracking.[23] At the statutory level, privacy is fragmented across sector-specific regimes such as HIPAA (health),[24] COPPA (children),[25] and GLBA (financial data),[26] with enforcement largely by the Federal Trade Commission (FTC). Absence of a federal omnibus law creates significant regulatory gaps.

Meanwhile, national security surveillance remains entrenched under the Foreign Intelligence Surveillance Act (FISA),[27] the Patriot Act,[28] and Section 702 of the FISA Amendments Act 2008,[29] authorising warrantless foreign-intelligence collection. Proceedings before the FISA Court occur ex parte and remain classified, limiting

19. *Consolidated Version of the Treaty on European Union* art. 4(2), 2016 O.J. (C 202) 1.

20. Orla Lynskey, *The Foundations of EU Data Protection Law*, 132, (Oxford Univ. Press 2015)

21. U.S. Const. amend. IV (protecting individuals' privacy against unreasonable searches and seizures)

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

23. *Carpenter v. United States*, 585 U.S. ___ (2018)

24. 45 C.F.R. pts. 160–164 (Health Insurance Portability and Accountability Act)

25. 15 U.S.C. §§ 6501–6506 (Children's Online Privacy Protection Act).

26. 15 U.S.C. §§ 6801–6827 (Gramm-Leach-Bliley Act)

27. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885

28. USA Patriot Act of 2001, § 215.

29. FISA Amendments Act of 2008, § 702.

transparency.[30] Post-Snowden reforms under the "USA FREEDOM" Act 2015 curtailed bulk metadata retention but left core programs intact, and as Donohue and Richards observe, the U.S. model privileges freedom of expression and innovation over data protection, yielding a "constitutional democracy of privacy without a general law of privacy."[31]

*India: From Constitutional Recognition to Statutory Retrenchment*

India's privacy jurisprudence transformed with *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), where a nine-judge bench held that privacy is intrinsic to Article 21's right to life and liberty[32] The Court drew on comparative constitutionalism and international norms, notably Article 17 ICCPR, to ground privacy in dignity and autonomy[33] In the Aadhaar judgment (2018), the Supreme Court upheld the biometric identification scheme but required procedural safeguards such as purpose limitation and restricted data sharing.[34] Critics argue, however, that extensive data linking across welfare and finance sectors undermines meaningful consent.[35]

The Digital Personal Data Protection Act 2023 (DPDPA) aims to codify data rights but grants the government sweeping exemptions under Section 17 for reasons of national security and public order.[36] The Data Protection Board of India lacks the structural independence that is characteristic of the EU's supervisory authorities.[37] Meanwhile, India's growing surveillance architecture, including facial recognition, the Central Monitoring System, and frequent internet shutdowns, reflects

30. Ralph Clarke, FISA Court and the Problem of Secret Oversight, 53 Wake Forest L. Rev. 375 (2019).

31. Laura Donohue, *The Cost of Counterterrorism: Power, Politics and Liberty,* 185 (Cambridge Univ. Press 2008).

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

33. International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

34. *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 S.C.C. 1 (India)

35. Upendra Baxi, Aadhaar and the Future of Privacy, 61 *Indian J. of Public Administration* 23 (2019).

36. Digital Personal Data Protection Act 2023, § 17 (India).

37. Gautam Ghosh, The DPDPA and the Future of Data Governance in India, 12 *Indian J. L. & Tech.* 45 (2024).

weak accountability.[38] India's model has thus been described as a "constitutional promise undermined by statutory pragmatism."[39]

*China: Privacy as a Managed Value in a Security State*

China's data regime is defined by comprehensive state surveillance through facial recognition, biometric tracking, and the Social Credit System.[40] The Personal Information Protection Law (PIPL, 2021)[41] and Data Security Law (DSL, 2021)[42] mirror the GDPR's structure, outlining consent and data minimisation, yet primarily serve national security goals. Both laws mandate data localisation and empower the Cyberspace Administration of China (CAC) as regulator under the State Council, reflecting centralized Party control over regulatory agencies.[43]

Judicial oversight remains limited. The National Intelligence Law 2017 obliges all organisations to cooperate with state intelligence work, effectively subordinating privacy to national security.[44] Courts rarely adjudicate privacy claims against public authorities, and civil society lacks autonomy to litigate surveillance abuses.[45] As Qin notes, China's legal architecture transforms data governance into an instrument of political stability rather than a domain of rights.[46] Consequently, privacy operates as a managed administrative value rather than an enforceable constitutional guarantee.

*Cross-cutting Themes and Comparative Lessons*

A comparative analysis of privacy and surveillance across the European Union, United States, India, and China reveals a set of recurring tensions that transcend jurisdictional boundaries. These themes expose

38. Siddharth Rathi, Surveillance and Internet Shutdowns in India, 17 *J. of Human Rights Practice* 71 (2022).

39. Ankit Kumar, Constitutional Privacy and the Administrative State in India, 41 *Oxford Human Rights Hub J.* 12 (2023).

40. Feng Liang et al., Constructing a Data-Driven Society: China's Social Credit System as a State Innovation, 10 *Policy & Internet* 415 (2018).

41. Personal Information Protection Law 2021 (China)

42. Data Security Law 2021 (China)

43. Cyberspace Administration of China, State Council, Regulations on Cybersecurity Management (2022).

44. National Intelligence Law 2017 (China) art. 7.

45. Tian Dai, Authoritarian Legality and Data Control in China, 27 *Info. & Comm. Tech. L.* 156 (2023).

46. Yulin Qin, Rule by Data: The Chinese Legal Architecture of Digital Governance, 15 *J. of Comparative L.* 101 (2022).

the structural dilemmas of governing digital societies in which data has become both an instrument of governance and a commodity of power.

The tension between security and rights remains the central fault line as every jurisdiction justifies expansive surveillance in the language of necessity as counter-terrorism, cybersecurity, or, more recently, public health. The COVID-19 pandemic normalised state access to mobility and health data through contact-tracing applications and emergency decrees, reinforcing the perception that security and efficiency may override autonomy.[47] The European Union's proportionality-based jurisprudence under Articles 7–8 of the *Charter of Fundamental Rights*[48] seeks to balance collective protection and individual rights, yet even it permits national-security derogations under Article 4(2) TEU.[49] The United States continues to privilege intelligence imperatives under the *Foreign Intelligence Surveillance Act* (FISA)[50] and its Section 702 amendments, while India and China routinely invoke sovereignty and security to legitimise large-scale data collection.[51] Across systems, the post-2020 era demonstrates how security rationales have been constitutionalised, reframing privacy as a conditional rather than absolute right.

Judicial review functions as the principal constraint on surveillance but with striking variance in intensity. The Court of Justice of the European Union (CJEU) and European Court of Human Rights (ECHR) have elaborated robust proportionality standards in cases such as *Schrems II* and *Big Brother Watch v. United Kingdom*.[14] India's Supreme Court in *K.S. Puttaswamy v. Union of India* constitutionalised privacy as part of Article 21's protection of life and liberty,[29] though subsequent enforcement has been uneven. U.S. courts, while historically protective of liberty under *Katz v. United States*[17] and *Carpenter v. United States*,[18] often defer to executive claims of national security and state secrecy.[11] In China, judicial review is effectively absent: courts operate within a vertically integrated Party-state structure that prioritises social management over individual redress. In this sense, the asymmetry of oversight mirrors each system's constitutional design; robust where rights are judicially entrenched and minimal where political control dominates.

---

47. Graham Greenleaf & Gregory Watts, COVID-19 and Surveillance: Democracy, Liberty and Public Health, 44 *UNSW L.J.*349 (2021).

48. *Charter of Fundamental Rights of the European Union* arts. 7–8, 2012 O.J. (C 326) 391.

49. *Consolidated Version of the Treaty on European Union* art. 4(2), 2016 O.J. (C 202) 1.

50. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885.

51. Digital Personal Data Protection Act 2023, § 17 (India), National Intelligence Law 2017, art. 7 (China).

A further convergence lies in public–private entanglement. Technology corporations such as Google, Meta, and ByteDance now function as de facto agents of state surveillance, collecting and monetising personal data at unprecedented scale. Governments, in turn, co-opt these infrastructures for intelligence, predictive policing, and administrative efficiency. This blurs the boundary between private consent and public compulsion, generating a hybrid ecosystem of control. The result is a fragmented global privacy order. The absence of harmonised international standards enables "privacy arbitrage,[52]" with data flowing toward jurisdictions offering weaker safeguards or broader exemptions. Cultural and ideological factors deepen this divergence: collectivist systems such as China legitimize pervasive monitoring in the name of stability, while liberal democracies valorise autonomy yet struggle to restrain security exceptionalism.

Collectively, these patterns reveal a global paradox: privacy is universally affirmed as a right yet persistently compromised in practice. The future challenge lies not merely in legislating safeguards, but in redefining legitimacy within a governance model where surveillance itself has become infrastructural.

## IV. THE ADEQUACY OF INTERNATIONAL HUMAN RIGHTS LAW

Existing international human rights instruments provide a foundational yet incomplete framework for regulating mass surveillance. The International Covenant on Civil and Political Rights (ICCPR), adopted in 1966, enshrines the right to privacy under Article 17, prohibiting arbitrary or unlawful interference with correspondence and family life. However, the treaty was drafted in a pre-digital era and offers no explicit guidance on matters such as data processing, algorithmic profiling, or cross-border information flows.[53] The Human Rights Committee's General Comment No. 16 interprets Article 17 broadly but remains largely hortatory, leaving significant discretion to states.[54]

Regional systems have advanced further but face similar structural limits. The European Court of Human Rights and the Inter-American Court of Human Rights have extended privacy protection to

52. the exploitation of differences in privacy knowledge, expectations, or legal protections to extract economic value from personal data without providing commensurate transparency, control, or compensation to the data subject (Acquisti, 2015; Acquisti et al., 2016)

53. Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 Harv. Int'l L.J. 81 (2015).

54. UN Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), ¶¶ 1–10, U.N. Doc. HRI/GEN/1/Rev.9 (Apr. 8, 1988).

surveillance contexts, yet enforcement depends on state compliance rather than coercive authority.[55] UN treaty bodies and Special Rapporteurs issue important normative guidance, including reports by the UN Special Rapporteur on the Right to Privacy from digital surveillance, but their findings are recommendations, not binding.[56]

Recognising these deficiencies, new multilateral initiatives have emerged. The proposed UN Global Digital Compact aims to establish shared principles for digital governance and privacy, including oversight of surveillance technologies.[57] The Council of Europe's Convention 108+ (2018) represents the only binding international instrument specifically addressing data protection, covering algorithmic processing and transborder data flows.[58] Similarly, the OECD Privacy Guidelines (2022) and G20 AI Principles (2019) articulate non-binding standards on transparency, proportionality, and accountability in automated decision-making.[59]

Yet without enforceable duties, such frameworks risk remaining aspirational. Scholars have therefore urged a recalibration of international law towards binding obligations governing state surveillance, modelled on the proportionality and necessity principles central to European and Indian jurisprudence.[60] The creation of an independent, treaty-based monitoring body with investigatory and quasi-judicial powers is akin to the Human Rights Committee or the European Data Protection Board and would mark a decisive step toward substantive oversight in the digital sphere.[61]

In essence, international law's normative foundation remains sound, but its institutional architecture has not kept pace with the technological developments of surveillance. The challenge is to translate principles of autonomy and dignity into enforceable, globally coordinated obligations.

---

55. *Weber & Saravia v. Germany*, App. No. 54934/00 (Eur. Ct. H.R. 2006).

56. UN Special Rapporteur on the Right to Privacy, Annual Report, U.N. Doc. A/HRC/49/55 (2022).

57. United Nations, Our Common Agenda: Towards a Global Digital Compact (2023).

58. Council of Europe, Convention 108+ for the Protection of Individuals with Regard to Automatic Processing of Personal Data (2018).

59. OECD, Privacy Guidelines on Transborder Flows of Personal Data (2022). G20, AI Principles (2019).

60. Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* 257–72 (Cambridge Univ. Press 2012).

61. Jeroen de Hert & Serge Gutwirth, Reinforcing International Oversight of Surveillance, 37 *Computer L. & Security Rev.*105 (2021).

## V. POLICY AND DOCTRINAL RECOMMENDATIONS

Moving forward, three policy priorities emerge. First, strengthening international oversight mechanisms remains imperative. The UN system may consider establishing a Special Rapporteur with quasi-binding authority or, more ambitiously, a Digital Rights Treaty Body dedicated to global surveillance and data protection.[62] Such an institution could consolidate reporting, harmonise standards, and issue binding interpretive rulings akin to those of the Human Rights Committee.

Second, comparative borrowing can accelerate normative convergence. The EU's GDPR offers a procedural template for consent, portability, and independent supervision, while India's *Puttaswamy* doctrine provides a rights-based foundation suited to Global South democracies.[63] These models should inform the drafting of a universal digital rights covenant grounded in dignity, proportionality, and accountability.

Third, the governance of AI-driven surveillance demands doctrinal innovation. States should codify four foundational principles: necessity, proportionality, transparency, and accountability.[64] Necessity requires demonstrable justification; proportionality ensures minimal intrusion; transparency mandates disclosure of algorithmic logic; and accountability establishes redress mechanisms for misuse.

In parallel, cross-border cooperation is essential to prevent "data havens" that exploit regulatory asymmetries. Bilateral or multilateral data adequacy agreements, inspired by the EU model, could mitigate vulnerabilities created by uneven protections across jurisdictions.[65] Finally, the role of civil society and NGOs should be institutionalised through participation rights in oversight proceedings, ensuring that privacy governance reflects democratic legitimacy rather than bureaucratic discretion.

Collectively, these measures would help evolve a coherent global privacy architecture, integrating normative ambition with institutional enforceability.

---

62. UN Human Rights Council, Report on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/54/37 (2023).

63. General Data Protection Regulation (EU) 2016/679.

64. UN Human Rights Committee, General Comment No. 34: Freedoms of Opinion and Expression ¶ 34 (2011).

65. David de Hert & V. Papakonstantinou, The EU and the USA: Adequacy, Safe Harbor and Beyond, 36 *Computer L. & Security Rev.* 105 (2020).

## VI. CONCLUSION

The comparative analysis underscores a universal paradox: privacy is constitutionally or rhetorically affirmed across legal systems, yet it remains persistently vulnerable to security exceptionalism and corporate overreach. The European Union demonstrates the potential of rights-based regulation, the United States reveals the resilience of judicial oversight amid statutory fragmentation, India embodies the tension between constitutional aspiration and administrative practice, and China exemplifies the dangers of unchecked surveillance power.

As mass surveillance becomes infrastructural, being embedded in health, security, and economic governance, the implications transcend individual privacy. What is at risk is the very architecture of democratic autonomy. International law must therefore reimagine its function: not merely as declaratory but as constitutive of digital legitimacy. A retooled global framework that is binding, enforceable, and rights-driven is essential to ensure that privacy remains a living condition of freedom in the data age, not a nostalgic ideal.

Ultimately, privacy is more than a right to seclusion; it is the foundation of autonomy, democracy, and human dignity. The defence of privacy, therefore, is the defence of the human condition in an age of total visibility.