TECHNOLOGY, PRIVACY, AND DATA PROTECTION: CONSTITUTIONAL RIGHTS & INTERNATIONAL STANDARDS

by

Shubhangi Pandey

ABSTRACT

The rapid evolution of technology has profoundly transformed the relationship between individuals, the state, and private actors, raising critical concerns about privacy and data protection. In an era defined by the digital economy, algorithmic governance, and pervasive surveillance, the protection of personal data has emerged as an essential component of constitutional rights and international human rights law. This paper explores the constitutional foundations of privacy, with a particular focus on India, and compares them with global jurisprudence in the United States, the United Kingdom, and the European Union. It further examines the development of international standards such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the European Union's General Data Protection Regulation (GDPR). Through an analysis of case law, legislation, and institutional frameworks, this research evaluates the tension between technological innovation and the protection of fundamental rights. The study argues that privacy, once viewed narrowly as a spatial right, has evolved into a multidimensional entitlement encompassing informational self-determination, autonomy, and dignity. The paper concludes by recommending harmonization of domestic constitutional protections with international norms to ensure effective safeguards against emerging threats posed by artificial intelligence, surveillance capitalism, and cross-border data flows.

Introduction

The twenty-first century has been characterized by the unprecedented expansion of digital technologies, including the internet, smartphones, biometric systems, and artificial intelligence. These technologies have become essential for governance, commerce, and social interaction, but they also present novel threats to personal autonomy and privacy. The collection, processing, and transfer of personal data have reached unparalleled scales, often beyond the comprehension or control of the individuals concerned. Consequently, the discourse on privacy and data protection has moved from the periphery of constitutional law to its very center, engaging courts, legislatures, and international organizations alike.

Privacy, as a constitutional and human right, was historically conceived as a protection against arbitrary state intrusion into the home. The famous articulation of the "right to be let alone" in *Samuel D. Warren & Louis D. Brandeis, The Right to Privacy* (1890) reflected this traditional understanding of spatial privacy.[1]Over time, however, courts and scholars have recognized that privacy is not limited to physical seclusion but also encompasses control over personal information, decisional autonomy, and dignity.[1] The emergence of the information society has thus reframed privacy as a multidimensional right with both negative and positive obligations upon the state.

In India, the jurisprudence on privacy culminated in the landmark *Justice K.S. Puttaswamy (Retd.) v. Union of India* case, where a nine-judge bench of the Supreme Court recognized privacy as a fundamental right under Article 21 of the Constitution.[2]The Court emphasized that privacy is intrinsic to dignity and liberty, thereby aligning Indian constitutional law with international human rights standards. This recognition came at a critical juncture when the state was expanding biometric identification through Aadhaar and when private corporations were increasingly commodifying personal data.

The scale of India's biometric identification programme underscores what was at stake in this recognition. Since its inception in 2009, the Unique Identification Authority of India has issued more than 1.4 billion Aadhaar numbers, making it one of the largest identity systems in the world, so that even a modest error or breach rate is capable of affecting tens of millions of residents.[1]

The comparative perspective is equally illuminating. In the United States, the Fourth Amendment has historically served as the bedrock of privacy protections, though its interpretation has struggled to keep pace with technological advances. In *Carpenter v. United States*, the Supreme Court held that the warrantless acquisition of cell-site location information violated the Fourth Amendment, underscoring the need to adapt constitutional doctrine to the

---

[1] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

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

realities of digital surveillance.[3] Similarly, in the United Kingdom, the Human Rights Act 1998 incorporates the right to respect for private and family life under Article 8 of the European Convention on Human Rights, thereby embedding privacy within domestic law. The European Union, through the GDPR, has gone further by establishing comprehensive standards for data protection and recognizing data privacy as both a consumer right and a fundamental right.

At the international level, privacy is explicitly enshrined in Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[1]These provisions impose obligations on states to prevent arbitrary interference with personal life and to ensure effective remedies for violations. The United Nations Human Rights Committee has elaborated that data protection is an integral aspect of the right to privacy, particularly in the context of mass surveillance and digital communication. Regional human rights systems, such as the Inter-American Court of Human Rights, have also increasingly emphasized the necessity of protecting data in the digital age.

This interplay between constitutional frameworks and international norms highlights both convergence and divergence. While there is broad consensus that privacy is a fundamental human right, the scope, limitations, and enforcement mechanisms vary significantly across jurisdictions. For instance, the U.S. continues to rely heavily on a sectoral approach and judicial interpretation, whereas the EU has adopted a regulatory model that places proactive obligations on data controllers. India, meanwhile, stands at a critical juncture, having constitutionally recognized privacy but still developing its statutory architecture through instruments like the Digital Personal Data Protection Act, 2023.

Technological challenges further complicate this legal landscape. Surveillance technologies, data analytics, artificial intelligence, and cross-border data transfers create new forms of vulnerability. The commodification of personal data in the digital economy has been aptly described as "surveillance capitalism," where companies monetize user behavior and preferences.[4] States, too, increasingly deploy digital technologies for governance and security, often without adequate safeguards. The risk is that privacy protections may be eroded in the name of efficiency, innovation, or national security.

Against this backdrop, this paper investigates the evolving relationship between technology, privacy, and data protection through constitutional and international perspectives. It aims to provide a holistic analysis of how courts, legislatures, and international bodies have sought to reconcile technological innovation with the protection of fundamental rights. The study is guided by three central questions:

1. How have constitutional courts interpreted the right to privacy in light of technological changes?

[3] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

[4] Shoshana Zuboff, The Age of Surveillance Capitalism (2019).

2. To what extent do international standards shape domestic legal frameworks on privacy and data protection?
3. What reforms are necessary to harmonize national laws with international human rights obligations and to address emerging technological threats?

By engaging these questions, the paper seeks to contribute to the broader discourse on human rights in the digital age. Ultimately, it argues for the need to construct a global normative order that balances technological progress with the inviolability of individual dignity and autonomy.

Evolution of the Right to Privacy and Data Protection

1. Early Conceptions of Privacy

The idea of privacy is neither modern nor exclusively Western. Ancient civilizations recognized the importance of seclusion, secrecy, and personal autonomy in different ways. In classical Roman law, the *domus* represented not only physical shelter but also a private sphere shielded from public intrusion.[1] Similarly, in Indic traditions, privacy was implicit in notions of personal dignity and the sanctity of domestic life, as reflected in cultural and religious practices.[5] However, these early conceptions were primarily spatial and familial, concerned more with the inviolability of the household than with control over information.

The modern articulation of privacy emerged in response to industrialization, urbanization, and the rise of the mass press in the nineteenth century. The seminal essay by Samuel Warren and Louis Brandeis, *The Right to Privacy*, argued that the law must evolve to protect individuals from intrusive media and technological advances such as instant photography.[1] This formulation, emphasizing the "right to be let alone," became the foundation for subsequent legal developments.

2. Privacy as a Constitutional and Human Right

The recognition of privacy as a constitutional right was initially piecemeal. In the United States, the Constitution does not explicitly mention privacy. Nonetheless, the Supreme Court gradually read privacy into various amendments. For instance, in *Griswold v. Connecticut*, the Court struck down a state law banning contraceptives, recognizing a right to marital privacy derived from the "penumbras" of the Bill of Rights[6]. Later cases, such as *Roe v. Wade*, extended privacy to decisional autonomy in reproductive matters.[1]

In contrast, European traditions explicitly linked privacy with dignity and autonomy. The European Convention on Human Rights (ECHR) in Article 8 guarantees the right to respect for private and family life, home, and correspondence.[7] This formulation explicitly recognizes both informational and decisional aspects of privacy, requiring states to ensure not only negative

---

[5] See Usha Ramanathan, A Human Rights Perspective on Privacy, in *Privacy Matters* 23 (2004).

[6] *Griswold v. Connecticut*, 381 U.S. 479 (1965).

[7] European Convention on Human Rights art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

obligations (non-interference) but also positive duties (protection from third-party intrusion). The jurisprudence of the European Court of Human Rights has further refined this understanding, particularly in cases addressing surveillance and data retention.[1]

The Indian constitutional framework initially lacked explicit recognition of privacy. In *M.P. Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of Uttar Pradesh* (1963), the Supreme Court denied that privacy constituted a fundamental right.[8] However, subsequent jurisprudence, particularly *Gobind v. State of Madhya Pradesh* (1975), cautiously acknowledged privacy as an element of personal liberty under Article 21.[1] This doctrinal evolution culminated in *Puttaswamy* (2017), where the Supreme Court explicitly declared privacy a fundamental right intrinsic to life and liberty, aligning Indian constitutional law with international norms.

3. Informational Privacy and Data Protection

The advent of the digital age shifted the focus from spatial and decisional privacy to informational privacy. Informational privacy concerns the right of individuals to control the collection, use, and dissemination of their personal data. This shift reflects the increasing importance of personal information in both economic and political domains.

Alan Westin, in his landmark work *Privacy and Freedom*, described privacy as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[9] This conceptualization directly informed later developments in data protection law. By the 1970s, several jurisdictions recognized that automated data processing created unique threats requiring specialized safeguards. The Organization for Economic Cooperation and Development (OECD) issued its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980, establishing foundational principles such as data quality, purpose limitation, and accountability.[1]

In Europe, the right to data protection developed into a distinct legal category. The Charter of Fundamental Rights of the European Union recognizes the right to data protection separately from the right to privacy, under Article 8.[10] This distinction acknowledges that informational autonomy requires specific protections beyond general privacy guarantees. The EU Data Protection Directive (1995) and its successor, the GDPR (2018), institutionalized this approach, creating comprehensive obligations for data controllers and processors.

India has also begun to grapple with informational privacy in the context of mass data collection through Aadhaar and digital governance systems. The Supreme Court in *Puttaswamy II* (2018) upheld Aadhaar but simultaneously emphasized the need for robust data protection legislation.[1] This tension reflects the global challenge of balancing innovation with fundamental rights.

---

[8] *M.P. Sharma v. Satish Chandra*, 1954 SCR 1077 (India); *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India).

[9] Alan F. Westin, Privacy and Freedom 7 (1967).

[10] Charter of Fundamental Rights of the European Union art. 8, 2000 O.J. (C 364) 1.

4. From National Frameworks to International Norms

The globalization of information flows necessitated the development of international standards. The Council of Europe's Convention 108 (1981) was the first binding international treaty on data protection, establishing common principles for member states.[11] At the United Nations level, Article 17 of the ICCPR imposes obligations on states to prevent arbitrary or unlawful interference with privacy. The UN Human Rights Committee has interpreted this provision to encompass data protection, particularly in contexts of surveillance and digital communication.[1]

Furthermore, the jurisprudence of regional human rights bodies has expanded the scope of privacy. The Inter-American Court of Human Rights, in its Advisory Opinion OC-23/17, explicitly recognized the right to data protection as part of the right to privacy under Article 11 of the American Convention on Human Rights.[12] Similarly, the African Union Convention on Cyber Security and Personal Data Protection (2014) demonstrates the growing recognition of informational privacy in diverse legal systems.

5. Emerging Challenges and Theoretical Shifts

Technological innovation has outpaced traditional legal frameworks, creating new challenges for privacy and data protection. The rise of artificial intelligence, machine learning, and predictive analytics has enabled unprecedented forms of surveillance and profiling. Scholars such as Shoshana Zuboff have described this as "surveillance capitalism," where personal data becomes a raw material for economic exploitation.[1]

The regulatory consequences of this model became apparent in May 2023, when Ireland's Data Protection Commission fined Meta Platforms Ireland Limited €1.2 billion for unlawfully transferring the personal data of European users to the United States, the largest penalty issued under the GDPR to date. The size of the fine illustrates how deeply transnational data flows have become embedded in the business models that Zuboff describes.[13]

At the same time, the conceptualization of privacy itself is shifting. While earlier theories emphasized individual control, contemporary scholarship highlights the relational and collective dimensions of privacy. Information about one individual often implicates others, and large-scale data practices affect democratic institutions as much as personal autonomy. This broader perspective underscores the need to frame privacy not merely as an individual right but as a public good essential for democracy, equality, and human dignity.

Constitutional Foundations of Privacy in India

---

[11] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, ETS No. 108.

[12] *Advisory Opinion OC-23/17*, Inter-Am. Ct. H.R. (Nov. 15, 2017).

[13] 'Meta Fined Record $1.3 Billion Over EU User Data Transfers to US' NBC News (22 May 2023) <https://www.nbcnews.com/news/world/meta-fined-record-13-billion-eu-user-data-transfers-us-rcna85515> accessed 26 July 2026.

1. Early Judicial Reluctance

The Indian Constitution, unlike some modern constitutions, does not explicitly enumerate a right to privacy. Consequently, the recognition of privacy has been left to judicial interpretation under the broad ambit of fundamental rights. In its early years, the Supreme Court of India was hesitant to acknowledge privacy as a constitutional entitlement.

In *M.P. Sharma v. Satish Chandra* (1954), the Court rejected a challenge to search and seizure provisions, holding that the Constitution did not recognize a right to privacy comparable to the Fourth Amendment of the United States Constitution.[1] The Court emphasized that the framers had deliberately omitted such a right and that Article 20(3) (protection against self-incrimination) and Article 19(1)(f) (right to property, since repealed) did not implicitly confer privacy guarantees.

Similarly, in *Kharak Singh v. State of Uttar Pradesh* (1963), the Court considered the constitutionality of police surveillance regulations.[14] The majority struck down domiciliary visits as unconstitutional but denied that privacy constituted a fundamental right. Justice Subba Rao's dissent, however, argued that privacy was integral to personal liberty under Article 21. His reasoning would later influence the trajectory of privacy jurisprudence.

2. Transitional Phase: Implicit Recognition of Privacy

Despite these early setbacks, later decisions began to recognize facets of privacy under the rubric of Article 21 (right to life and personal liberty). In *Gobind v. State of Madhya Pradesh* (1975), the Court cautiously accepted that privacy could be a fundamental right, though subject to reasonable restrictions.[1] The Court drew upon comparative jurisprudence and acknowledged that privacy includes the right to safeguard personal intimacies, family life, and personal identity.

This reasoning was further advanced in *R. Rajagopal v. State of Tamil Nadu* (1994), popularly known as the "Auto Shankar case."[15] The Court held that the right to privacy encompasses the right to prevent unauthorized publication of one's life story, recognizing a dimension of informational privacy. Similarly, in *People's Union for Civil Liberties (PUCL) v. Union of India* (1997), the Court struck down phone tapping provisions lacking procedural safeguards, affirming that the right to privacy protects communications.[1]

These cases collectively laid the groundwork for the full constitutional recognition of privacy, albeit without an explicit doctrinal foundation.

3. Puttaswamy and the Recognition of Privacy as a Fundamental Right

The turning point came in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), where a nine-judge bench unanimously declared privacy a fundamental right under Part III of the

---

[14] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India)
[15] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 (India)

Constitution.[16] The Court overruled *M.P. Sharma* and *Kharak Singh* to the extent they denied privacy.

Justice D.Y. Chandrachud's plurality opinion described privacy as intrinsic to life and liberty under Article 21, while also flowing from the guarantees of equality (Articles 14 and 15) and freedoms (Article 19). The Court emphasized that privacy is not merely a negative right against intrusion but a positive entitlement that safeguards autonomy, dignity, and informational self-determination.

The judgment identified three strands of privacy: (i) spatial privacy (freedom from physical intrusion), (ii) decisional autonomy (choices regarding marriage, sexuality, procreation), and (iii) informational privacy (control over personal data).[1] This multidimensional framework aligned Indian jurisprudence with comparative constitutional and international standards.

The Court also underscored the relationship between privacy and other fundamental rights. For example, it noted that without privacy, freedoms of expression and association may be chilled by surveillance, and equality may be undermined if personal information is used to discriminate. By framing privacy as a structural principle of constitutional governance, *Puttaswamy* ensured its enduring significance.

4. Aadhaar and the Limits of Privacy

The recognition of privacy as a fundamental right soon faced its first major test in the Aadhaar litigation. In *K.S. Puttaswamy v. Union of India (Aadhaar Case)* (2018), a five-judge bench upheld the constitutionality of Aadhaar while imposing restrictions.[17] The Court reasoned that Aadhaar's purpose of ensuring targeted delivery of welfare benefits served a legitimate state interest, and that data protection measures within the Aadhaar framework provided sufficient safeguards.

However, the Court struck down provisions permitting private entities to demand Aadhaar authentication, citing risks of excessive data aggregation.[1] Justice Chandrachud, in his dissent, argued that Aadhaar violated privacy by enabling pervasive surveillance and failing to ensure robust data protection. His dissent has since been lauded for emphasizing informational self-determination and technological accountability.

The human cost of this tension is illustrated by welfare exclusion linked to Aadhaar authentication. The Right to Food Campaign has documented dozens of starvation-related deaths across several Indian states since 2015 in which failures of biometric authentication, or the absence of Aadhaar linkage, contributed to the denial of subsidised rations, with children and elderly persons disproportionately affected. These accounts suggest that the Court's

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

[17] *K.S. Puttaswamy v. Union of India* (Aadhaar Case), (2019) 1 SCC 1 (India).

emphasis on proportionality has not, in practice, been matched by adequate operational safeguards at the point of service delivery.[18]

The Aadhaar case illustrates the complex balancing of privacy with state interests in welfare delivery and national security. While recognizing privacy's constitutional stature, the Court demonstrated judicial deference to legislative policy, raising questions about the robustness of privacy protections in practice.

5. Statutory Developments: Towards a Data Protection Framework

The recognition of privacy as a fundamental right created an imperative for comprehensive legislation on data protection. The Justice B.N. Srikrishna Committee, constituted in 2017, submitted its report along with a draft Personal Data Protection Bill in July 2018, drawing inspiration from the GDPR.[1] After years of debate, Parliament enacted the **Digital Personal Data Protection Act, 2023 (DPDPA)**.[19]

The DPDPA establishes principles of purpose limitation, data minimization, and user consent. It creates obligations for data fiduciaries and introduces penalties for non-compliance. However, the Act has been criticized for broad exemptions granted to the state, limited independence of the Data Protection Board, and ambiguous provisions on cross-border data transfers.[1] Critics argue that these features dilute constitutional protections and fail to fully implement the vision articulated in *Puttaswamy*.

Parallel to this, sectoral regulations, such as the Information Technology Act, 2000 and its rules on sensitive personal data, continue to operate, but they lack the comprehensive scope of the DPDPA. Together, these frameworks indicate India's incremental progress towards aligning statutory law with constitutional mandates.

6. Privacy and Emerging Rights: Sexuality, Identity, and Dignity

The recognition of privacy has also transformed other domains of constitutional rights. In *Navtej Singh Johar v. Union of India* (2018), the Supreme Court struck down Section 377 of the Indian Penal Code, decriminalizing consensual same-sex relations.[20] The Court relied heavily on privacy, autonomy, and dignity, building upon *Puttaswamy*. Similarly, in *Joseph Shine v. Union of India* (2018), adultery was decriminalized on grounds of dignity and autonomy, again linking privacy to substantive equality.[1]

---

[18] Scroll Staff, 'A Year After Jharkhand Girl Died of Starvation, Aadhaar Tragedies Are on the Rise' Scroll.in (25 January 2019) <https://scroll.in/article/895667/a-year-after-jharkhand-girl-died-of-starvation-aadhaar-tragedies-are-on-the-rise> accessed 26 July 2026.

[19] The Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India)

[20] *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1 (India).

These cases demonstrate that privacy is not merely about data or surveillance but about the core of individual identity and choice. Privacy jurisprudence in India thus reflects a broader constitutional transformation towards substantive liberty and equality.

7. Critical Reflections

Despite its progressive trajectory, Indian privacy jurisprudence faces several challenges. First, the Supreme Court's recognition of privacy has not always translated into robust protection in practice, as seen in the Aadhaar case. Second, legislative frameworks like the DPDPA leave wide leeway for executive discretion, risking disproportionate state intrusion. Third, enforcement mechanisms remain weak, with limited institutional capacity for oversight.

Moreover, the Indian context presents unique challenges due to its scale, diversity, and socio-economic disparities. Ensuring meaningful consent in a country with significant digital illiteracy is particularly difficult. This concern is borne out by connectivity data: a 2024 industry analysis found that only around 52 per cent of India's population were active internet users, leaving close to half the country offline, with usage considerably lower in poorer and rural households. Meaningful consent is difficult to obtain from data principals who lack basic digital access, let alone the literacy required to understand consent notices.[21] Similarly, balancing welfare delivery with data protection remains a pressing dilemma. These challenges highlight the need for stronger institutional safeguards, greater transparency, and alignment with international best practices.

Comparative Constitutional Perspectives

The recognition of privacy as a fundamental right has not followed a uniform path across jurisdictions. Different constitutional systems have conceptualized privacy in distinct ways, reflecting their historical traditions, institutional structures, and socio-political priorities. This section examines the constitutional approaches of the United States, the United Kingdom, and the European Union, and contrasts them with Indian jurisprudence.

1. The United States: Privacy Through Constitutional Interpretation

The United States Constitution does not explicitly recognize a right to privacy. Instead, American courts have derived privacy protections through judicial interpretation of various provisions of the Bill of Rights. The most influential articulation came in *Griswold v. Connecticut* (1965), where the Supreme Court struck down a ban on contraceptives, reasoning that privacy emanated from the "penumbras" and "emanations" of specific constitutional guarantees.[1]

The Court extended this reasoning in *Roe v. Wade* (1973), recognizing a woman's right to choose abortion as part of privacy and liberty.[22] However, this jurisprudence has been contested

[21] Simon Kemp, 'Digital 2024: India' (DataReportal, 23 February 2024) <https://datareportal.com/reports/digital-2024-india> accessed 26 July 2026.

[22] *Roe v. Wade*, 410 U.S. 113 (1973)

and was ultimately overturned in *Dobbs v. Jackson Women's Health Organization* (2022), reflecting the fragility of privacy-based decisional autonomy in the U.S.[1]

Apart from decisional autonomy, American jurisprudence has also addressed privacy in the context of surveillance and information. The Fourth Amendment protects against unreasonable searches and seizures, and its application has been tested in the digital age. In *Katz v. United States* (1967), the Court held that privacy depends not on physical intrusion but on a "reasonable expectation of privacy."[23] More recently, in *Carpenter v. United States* (2018), the Court extended Fourth Amendment protections to cell-site location data, recognizing that digital surveillance posed unique threats.[1]

The U.S. has generally adopted a sectoral approach to data protection, with statutes regulating specific domains such as health (HIPAA), finance (GLBA), and children's online privacy (COPPA). There is no comprehensive federal data protection law akin to the EU's GDPR.[24] This fragmentation has increasingly been filled by state legislatures rather than Congress. By late 2025, nineteen U.S. states, including California, Virginia, Colorado, and Texas, had enacted comprehensive consumer privacy statutes of their own, while successive proposals for a comprehensive federal law, most recently the American Privacy Rights Act, have repeatedly stalled in Congress.[1] This fragmented regime often leaves individuals vulnerable to inconsistent protections, especially in the era of big data and artificial intelligence.

2. The United Kingdom: Privacy through Human Rights Incorporation

The United Kingdom, with its unwritten constitution, traditionally relied on common law remedies such as trespass and breach of confidence to address privacy concerns. For much of its history, the U.K. courts were reluctant to recognize privacy as a standalone right.

This changed with the enactment of the Human Rights Act 1998 (HRA), which incorporated the European Convention on Human Rights into domestic law. Article 8 of the ECHR provides for the right to respect for private and family life, home, and correspondence.[25] Through the HRA, individuals gained the ability to invoke Article 8 in U.K. courts, thereby embedding privacy protections within domestic constitutional law.

Notable cases such as *Campbell v. MGN Ltd.* (2004) illustrate this development. In that case, the House of Lords recognized that the publication of private medical information violated Article 8, balancing privacy against freedom of expression under Article 10.[1] The case demonstrated how U.K. courts integrated European human rights principles into common law doctrines.

---

[23] *Katz v. United States*, 389 U.S. 347 (1967)

[24] See Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law* 57–64 (7th ed.2021)

[25] European Convention on Human Rights art. 8, Nov. 4, 1950, 213 U.N.T.S. 221

Data protection in the U.K. has been shaped significantly by EU law. The Data Protection Act 1998 implemented the EU Data Protection Directive, while the Data Protection Act 2018 aligns with the GDPR.[26] After Brexit, the U.K. retained a similar framework, though questions remain about adequacy in cross-border transfers with the EU.

The U.K. approach emphasizes balancing individual rights with public interest, particularly in contexts of national security and surveillance. The Investigatory Powers Act 2016, often referred to as the "Snooper's Charter," has been criticized for granting broad surveillance powers, though subject to judicial and parliamentary oversight.[1]

3. The European Union: Privacy and Data Protection as Fundamental Rights

The European Union represents the most comprehensive framework for privacy and data protection globally. Unlike the U.S. or U.K., the EU explicitly recognizes data protection as a fundamental right. Article 7 of the Charter of Fundamental Rights guarantees respect for private and family life, while Article 8 separately affirms the right to the protection of personal data.[27]

The General Data Protection Regulation (GDPR), effective since 2018, operationalizes these rights through detailed obligations for data controllers and processors. The GDPR embodies principles of lawfulness, fairness, transparency, purpose limitation, data minimization, and accountability. It also provides individuals with enforceable rights, including the right to access, rectification, erasure ("right to be forgotten"), and data portability.[1]

EU jurisprudence has played a key role in shaping global privacy standards. In *Google Spain SL v. Agencia Española de Protección de Datos* (2014), the Court of Justice of the European Union (CJEU) recognized the right to be forgotten, requiring search engines to delist outdated or irrelevant information.[28] In the *Schrems* cases, the CJEU invalidated data transfer agreements with the U.S. (Safe Harbor and Privacy Shield), citing inadequate protection of EU citizens' data from U.S. surveillance.[1]

The EU's approach reflects a proactive regulatory model that prioritizes individual control and accountability. Unlike the sectoral approach in the U.S., the GDPR establishes uniform standards across all sectors and member states, making it a global benchmark.

4. Comparative Reflections: India and Global Trends

India's constitutional recognition of privacy in *Puttaswamy* (2017) reflects both convergence and divergence with these comparative models. Like the U.S., India's Constitution does not explicitly mention privacy, and its recognition has emerged through judicial interpretation. However, unlike the U.S., where privacy rights remain contested and fragmented, India has

[26] Data Protection Act 2018, c. 12 (U.K.)

[27] Charter of Fundamental Rights of the European Union arts. 7–8, 2000 O.J. (C 364) 1

[28] *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, ECLI:EU:C:2014:317

constitutionally entrenched privacy as a fundamental right with a broad multidimensional scope.

In comparison with the U.K., India's approach is less reliant on international incorporation and more grounded in constitutional interpretation. Yet, similar to the U.K., India grapples with balancing privacy against state surveillance and welfare delivery, as seen in the Aadhaar litigation.

Relative to the EU, India's statutory framework lags behind. While the GDPR offers comprehensive protections and independent enforcement, India's Digital Personal Data Protection Act, 2023 provides a narrower scope, broad state exemptions, and limited institutional independence. The absence of a strong, autonomous data protection authority contrasts with the EU's robust enforcement mechanisms.

A critical lesson from these comparative perspectives is that the strength of privacy protections depends not only on judicial recognition but also on legislative design and institutional capacity. India's constitutional jurisprudence is progressive, but without effective statutory safeguards, privacy risks remain acute.

5. Emerging Global Convergence and Divergence

Despite differences, there are signs of convergence in global privacy norms. Most jurisdictions now recognize informational privacy as central to individual dignity and autonomy. The influence of the GDPR has been particularly strong, inspiring legislation in countries such as Brazil (LGPD), South Korea, and South Africa.[29] India's DPDPA also reflects GDPR principles, albeit with significant modifications.

However, divergence persists in balancing privacy with competing interests. The U.S. prioritizes innovation and national security, often at the expense of uniform privacy protections. The EU emphasizes individual rights and regulatory oversight, even at the cost of compliance burdens. India occupies a middle ground, seeking to balance digital governance, welfare delivery, and privacy, but with institutional and infrastructural limitations.

The comparative analysis underscores that privacy is not a static or uniform concept but one that evolves with legal culture, political priorities, and technological change.

International Human Rights Standards on Privacy and Data Protection

1. Privacy in the Universal Human Rights Framework

The right to privacy achieved global recognition in the aftermath of World War II, when human rights norms were codified in international instruments. Article 12 of the Universal Declaration of Human Rights (UDHR, 1948) declares:

[29]Lei Geral de Proteção de Dados Pessoais, Law No. 13,709, Aug. 14, 2018 (Braz.)

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[1]

This provision conceptualized privacy broadly, encompassing family life, communications, and reputation. Though the UDHR itself is not legally binding, it has shaped customary international law and inspired binding treaties.

The International Covenant on Civil and Political Rights (ICCPR, 1966) reinforces this commitment. Article 17 mirrors Article 12 of the UDHR, prohibiting arbitrary or unlawful interference with privacy, family, and correspondence.[30] The ICCPR imposes binding obligations on ratifying states to protect privacy not only from the state but also from private actors, requiring states to enact laws and remedies.

The Human Rights Committee, which oversees implementation of the ICCPR, elaborated in **General Comment No. 16 (1988)** that privacy encompasses "autonomy, identity, and the right to establish relationships."[1] The Committee also emphasized that states must regulate both state and non-state actors engaged in the processing of personal data. In its Concluding Observations on state reports, the Committee has criticized mass surveillance programs and weak data protection frameworks as inconsistent with Article 17.[31]

The UDHR and ICCPR together form the cornerstone of global privacy norms, establishing a broad right to be free from arbitrary interference and mandating effective protections in domestic law.

2. Privacy in Regional Human Rights Systems

Regional human rights regimes have significantly advanced privacy and data protection beyond the global framework.

(a) Europe

The **European Convention on Human Rights (ECHR, 1950)** in Article 8 guarantees the right to respect for private and family life, home, and correspondence.[1] The European Court of Human Rights (ECtHR) has developed a robust jurisprudence under Article 8, balancing privacy with legitimate aims such as national security, crime prevention, and public order.

In *Klass v. Germany* (1978), the ECtHR upheld surveillance measures but emphasized that secret surveillance must be subject to adequate safeguards against abuse.[32] In *S. & Marper v. United Kingdom* (2008), the Court held that indefinite retention of DNA data violated Article 8, recognizing informational privacy as integral to human dignity.[1] The Court has also

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

[31] Id. 8–10

[32] *Klass v. Germany*, 2 Eur. H.R. Rep. 214 (1978)

scrutinized bulk interception regimes, most recently in *Big Brother Watch v. United Kingdom* (2021), where it emphasized proportionality and independent oversight.[33]

Europe also pioneered binding data protection instruments. The **Convention 108 (1981)** of the Council of Europe was the first international treaty specifically addressing data protection, later modernized by **Convention 108+ (2018)** to account for digital technologies.[1] At the EU level, the Charter of Fundamental Rights (2000) recognizes privacy (Article 7) and data protection (Article 8) as distinct rights, giving rise to the GDPR.[34]

(b) Inter-American System

The **American Convention on Human Rights (ACHR, 1969)** protects privacy under Article 11, guaranteeing the right to dignity, honor, and protection against arbitrary interference.[1] The Inter-American Court of Human Rights (IACtHR) has given this provision an expansive interpretation.

In its **Advisory Opinion OC-23/17**, the IACtHR recognized the right to data protection as part of Article 11, affirming that informational self-determination is essential to democratic societies.[35] The Court stressed that states must regulate data collection, processing, and cross-border transfers, especially in light of digital technologies.

(c) African System

The **African Charter on Human and Peoples' Rights (1981)** does not explicitly mention privacy, but the African Court and Commission have interpreted provisions on dignity and freedom to encompass privacy.[1] More concretely, the **African Union Convention on Cyber Security and Personal Data Protection (2014)** (the Malabo Convention) establishes binding obligations for member states to regulate personal data, reflecting growing recognition of informational privacy on the continent.[36]

3. United Nations Special Procedures and Resolutions

In addition to treaties, the UN has advanced privacy standards through special procedures and resolutions. The Human Rights Council has repeatedly emphasized the importance of privacy in the digital age. Resolution 68/167 (2013), titled *The Right to Privacy in the Digital Age*, called upon states to review surveillance practices and ensure compliance with Article 17 of the ICCPR.[1]

---

[33] *Big Brother Watch v. United Kingdom*, 72 Eur. H.R. Rep. 17 (2021)

[34] Charter of Fundamental Rights of the European Union arts. 7–8, 2000 O.J. (C 364)

[35] *Advisory Opinion OC-23/17*, Inter-Am. Ct. H.R. (Nov. 15, 2017).

[36] African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014.

The creation of the **UN Special Rapporteur on the Right to Privacy (2015)** institutionalized global monitoring. The Special Rapporteur has highlighted risks posed by artificial intelligence, biometric systems, and surveillance capitalism, and has urged stronger safeguards for cross-border data flows.[37]

More recently, UN member states adopted the Global Digital Compact on 22 September 2024 as an annex to the Pact for the Future at the Summit of the Future in New York. Among its commitments, the Compact calls for advancing interoperable data governance approaches and safeguarding human rights online, representing the first comprehensive global framework of its kind, though its provisions remain non-binding and their translation into enforceable protections is still uncertain.[1]

The Office of the High Commissioner for Human Rights (OHCHR) has also published reports warning that indiscriminate surveillance and weak corporate accountability undermine not only privacy but also freedom of expression and assembly.[38]

4. Data Protection in International Trade and Cross-Border Data Flows

The globalization of digital commerce has raised privacy concerns in international trade law. Data flows underpin global supply chains, cloud services, and digital platforms, creating tensions between economic integration and data sovereignty.

The World Trade Organization (WTO) recognizes privacy as a legitimate ground for restricting cross-border trade under Article XIV of the General Agreement on Trade in Services (GATS).[1] Similarly, free trade agreements increasingly incorporate data protection clauses. The EU-Japan Economic Partnership Agreement, for instance, conditions data flows on adequacy decisions ensuring an equivalent level of protection.[39]

These developments indicate that privacy and data protection are no longer confined to human rights law but intersect with international economic law, reinforcing their global significance.

5. Key Challenges in the International Framework

Despite these advances, significant challenges remain:

1. **Enforcement gaps**: While global treaties recognize privacy, enforcement depends on domestic implementation. Many states lack effective oversight bodies or judicial remedies.

---

[37] U.N. Human Rights Council, Res. 28/16, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/RES/28/16 (Apr. 1, 2015).

[38] Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (June 30, 2014).

[39] EU-Japan Economic Partnership Agreement, 2019 O.J. (L 330) 3.

2. **Extraterritoriality**: The global nature of digital data flows raises questions about jurisdiction. The EU's GDPR asserts extraterritorial reach, but harmonization across jurisdictions remains limited.

3. **Surveillance practices**: Mass surveillance by powerful states often undermines international commitments. Revelations by Edward Snowden about the U.S. National Security Agency (NSA) highlighted the gap between formal obligations and actual practices.[1]

4. **Technological pace**: International law struggles to keep up with emerging threats from artificial intelligence, biometrics, and genetic data. The normative framework is often reactive rather than proactive.

6. Comparative Assessment with India

India is a party to the ICCPR and thus bound by Article 17 obligations.[40] The Supreme Court in *Puttaswamy* cited international instruments such as the UDHR and ICCPR to support its recognition of privacy as a fundamental right.[1] However, India's domestic framework lags behind international standards in several respects.

Unlike the EU, India does not recognize data protection as a separate constitutional right, though the DPDPA incorporates some GDPR-inspired principles. Furthermore, broad state exemptions under the DPDPA may conflict with India's obligations under the ICCPR to prevent arbitrary interference.

Regionally, India is not a party to Convention 108 or the Malabo Convention, limiting its engagement with binding international data protection norms. Nonetheless, India's participation in forums such as the G20 and its emphasis on digital governance underscore the need to align domestic law with global standards to ensure trust in cross-border data flows.

Technological Challenges and Emerging Threats

The recognition of privacy and data protection as fundamental rights has been accompanied by unprecedented technological transformations. Digital technologies have enabled new modes of communication, governance, and commerce, but they have also generated novel threats to individual autonomy, dignity, and security. The challenge for constitutional and international law lies in adapting normative frameworks to address these emerging risks.

---

[40] ICCPR, supra note 2.

1. Artificial Intelligence and Algorithmic Profiling

Artificial intelligence (AI) and machine learning systems rely heavily on large datasets, often containing sensitive personal information. These technologies enable predictive analytics, facial recognition, and automated decision-making, but they also raise concerns about opacity, bias, and discrimination.

For example, algorithmic profiling in credit scoring, recruitment, and law enforcement can entrench existing inequalities.41 The lack of transparency in "black box" algorithms undermines accountability and the ability of individuals to challenge adverse decisions. In the EU, the GDPR attempts to address this through Article 22, which grants individuals the right not to be subject to automated decisions with legal or significant effects.1 However, enforcement remains uneven, and most jurisdictions, including India, lack equivalent protections.

AI-driven surveillance systems, particularly facial recognition, pose acute privacy risks. In India, the deployment of the Automated Facial Recognition System (AFRS) for law enforcement has been criticized for lacking statutory safeguards.42 Right to Information requests filed by the Internet Freedom Foundation revealed that Delhi Police treats any facial recognition match above 80 per cent similarity as a positive result, a benchmark that international accuracy tests suggest is unreliable: a 2018 trial by the American Civil Liberties Union found that Amazon's Rekognition software incorrectly matched twenty-eight sitting members of the U.S. Congress with criminal mugshots at a similar confidence threshold. Such findings raise the possibility of wrongful identification without any accompanying statutory recourse in India.[1] Similar concerns have been raised in the United States, where studies demonstrate racial bias in facial recognition technologies.43 Without strict legal oversight, AI risks normalizing mass surveillance and discriminatory practices.

2. Biometrics and Identity Systems

Biometric technologies such as fingerprints, iris scans, and facial recognition are increasingly used for identification and authentication. While biometrics can enhance efficiency in service delivery, they also create unique risks because biometric data is immutable — once compromised, it cannot be changed like a password.

India's Aadhaar system exemplifies both the promise and perils of biometrics. Designed to provide a unique digital identity for residents, Aadhaar facilitates welfare delivery and financial inclusion.1 However, critics argue that its centralized architecture makes it vulnerable to

---

[41] See Solon Barocas & Andrew D. Selbst, Big Data's Disparate Impact, 104 Calif. L. Rev. 671, 678–82 (2016).

[42] Internet Freedom Foundation, Automated Facial Recognition System in India: A Legal and Policy Review (2020).

[43] Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proc. Machine Learning Res. 1 (2018).

misuse and surveillance.44 The Supreme Court in the Aadhaar Case upheld the scheme but emphasized restrictions on private sector use and mandated data protection safeguards.1 Yet breaches and unauthorized disclosures continue to raise serious concerns.

These concerns were reinforced in October 2023, when the cybersecurity firm Resecurity reported that the personal data, including Aadhaar and passport details, of an estimated 815 million Indians had appeared for sale on the dark web, allegedly linked to a breach of a government-run medical research database. The Unique Identification Authority of India disputed that its own systems had been compromised, underscoring the difficulty of assigning accountability within a complex, multi-agency data ecosystem.[45]

Globally, biometric databases have proliferated in border control, counter-terrorism, and civil registration systems. The European Union's Eurodac database for asylum seekers and the U.S. Department of Homeland Security's biometric programs illustrate the securitization of biometrics.1 The absence of global standards for biometric governance poses risks of abuse and cross-border misuse.

3. Surveillance Capitalism and Datafication

The commodification of personal data has become a defining feature of the digital economy. Shoshana Zuboff characterizes this phenomenon as "surveillance capitalism," where companies extract behavioral data to predict and influence user behavior.46 Platforms such as Google and Facebook monetize personal information through targeted advertising, raising questions about informed consent and autonomy.

This business model relies on pervasive tracking across devices, applications, and physical spaces. Techniques such as cookies, geolocation tracking, and behavioral analytics create detailed profiles that go far beyond the individual's awareness.1 Even when users consent to data collection, the asymmetry of knowledge and bargaining power renders such consent largely illusory.

This dynamic was starkly illustrated in 2019, when the U.S. Federal Trade Commission imposed a $5 billion penalty on Facebook, the largest privacy-related penalty levied by an American regulator at the time, for deceiving users about their ability to control the sharing of personal data with third-party applications such as Cambridge Analytica. The settlement required structural changes to Facebook's internal privacy governance, including an

---

[44] Usha Ramanathan, Aadhaar: From Welfare to Surveillance, 52 Econ. & Pol. Wkly. 7 (2017).

[45] 'Massive Aadhaar Data Breach of 815 Million Indians: Here's How to Keep Your Details Safe' Outlook Business (31 October 2023) <https://business.outlookindia.com/news/massive-aadhaar-data-breach-of-815-million-indians-heres-how-to-keep-your-details-safe> accessed 26 July 2026.

[46] Shoshana Zuboff, *The Age of Surveillance Capitalism* 8 (2019).

independent board committee, though critics observed that the penalty amounted to only a small fraction of the company's annual revenue.[47]

Regulatory responses vary. The GDPR imposes strict consent and transparency requirements, while the California Consumer Privacy Act (CCPA) grants rights to access and opt out of data sales.1 In India, the Digital Personal Data Protection Act, 2023 incorporates consent and purpose limitation principles but provides wide exemptions for government processing.48 Without robust enforcement, surveillance capitalism risks undermining both consumer protection and democratic accountability.

4. Cybersecurity and Data Breaches

The proliferation of digital data has heightened vulnerabilities to cybersecurity threats. Data breaches exposing sensitive information — from credit card details to health records — have become commonplace. Such breaches undermine trust in digital systems and can have severe consequences, including financial fraud, identity theft, and reputational harm.

High-profile incidents, such as the Equifax breach in the United States (2017) and the Aadhaar-related leaks in India, highlight systemic weaknesses in data security.1 The WannaCry ransomware attack (2017) demonstrated the global scale of cyber vulnerabilities, affecting hospitals, corporations, and public services worldwide.49

Constitutional and international frameworks often address cybersecurity indirectly through privacy and data protection norms. However, effective protection requires integrating data protection with cybersecurity governance. The Budapest Convention on Cybercrime (2001), though not universally ratified, remains the most significant international treaty addressing cyber threats.1 India, notably, is not a party, which limits its participation in global cooperation mechanisms.

5. Cross-Border Data Flows and Digital Sovereignty

The global nature of data flows raises complex jurisdictional and sovereignty issues. Cloud computing, global e-commerce, and transnational social media platforms mean that personal data routinely crosses borders. Ensuring consistent protection in such contexts is a formidable challenge.

---

[47] Federal Trade Commission, 'FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook' (FTC, 24 July 2019) <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook> accessed 26 July 2026.

[48] Federal Trade Commission, *Equifax Data Breach Settlement* (2019).

[49] Council of Europe, Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167.

The European Union's adequacy mechanism under the GDPR restricts transfers to jurisdictions with "essentially equivalent" protection.50 The invalidation of the EU–U.S. Privacy Shield in Schrems II illustrates the tensions between privacy and national security.1 The decision underscored that mass surveillance practices in the U.S. undermined the adequacy of protections for EU citizens' data.

The European Commission subsequently adopted a fresh adequacy decision for the EU-U.S. Data Privacy Framework on 10 July 2023, once again permitting personal data to flow to self-certified American organisations without additional safeguards such as standard contractual clauses. The Framework has already faced a legal challenge before the General Court of the European Union, suggesting that the underlying tension between EU privacy standards and U.S. surveillance law identified in Schrems II has been managed rather than definitively resolved.[51]

India has expressed concerns about "data colonization" and emphasized data localization in policy documents such as the Draft National E-Commerce Policy (2019).1 Proponents argue that localization enhances sovereignty, security, and regulatory control. Critics, however, warn that localization may fragment the internet, increase compliance costs, and hinder innovation.

Balancing cross-border flows with data sovereignty requires careful calibration. Overly restrictive policies risk economic isolation, while excessive openness may undermine constitutional rights. The absence of a coherent global framework remains a major gap in international governance.

6. Emerging Threats: Genetics, IoT, and Quantum Computing

Beyond AI and biometrics, emerging technologies present new frontiers for privacy. Genetic data, collected through medical research and commercial testing services, poses unique risks due to its deeply personal and familial implications. Internet of Things (IoT) devices, from smart homes to wearable technologies, continuously collect intimate behavioral data, often without meaningful user control.52

Looking forward, quantum computing may disrupt existing encryption systems, threatening the security of digital communications and data storage. Without proactive governance, these technologies may erode privacy protections even further.

7. Normative and Constitutional Challenges

---

[50] *Schrems II*, Case C-311/18, ECLI:EU:C:2020:559.

[51] McCann FitzGerald, 'European Commission Adopts Adequacy Decision for the New EU-US Data Privacy Framework' (McCann FitzGerald, 10 July 2023) <https://www.mccannfitzgerald.com/knowledge/data-privacy-and-cyber-risk/european-commission-adopts-adequacy-decision-for-the-new-eu-us-data-privacy-framework> accessed 26 July 2026.

[52] Scott R. Peppet, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85 (2014).

The technological landscape creates several normative dilemmas:

Consent and autonomy: Traditional consent models are ill-suited for pervasive and complex data processing.

Accountability: Algorithmic opacity challenges traditional mechanisms of legal accountability.

Equality: Discriminatory impacts of profiling and surveillance disproportionately affect marginalized communities.

Proportionality: Courts must grapple with applying proportionality analysis in the context of complex technological systems.

Constitutional courts, legislatures, and international bodies face the task of reinterpreting rights in light of these challenges. Privacy must be reconceptualized as not only an individual right but also a structural principle essential to democracy and social justice.

Judicial Developments and Landmark Cases

Courts have been instrumental in shaping the contours of privacy and data protection, often filling gaps left by legislatures. Judicial interpretations not only expand the scope of constitutional rights but also create normative frameworks that influence international standards. This section examines key judicial developments across jurisdictions.

1. India: From Reluctance to Robust Recognition

(a) Early Resistance

As noted earlier, the Indian Supreme Court initially denied privacy as a fundamental right. In *M.P. Sharma v. Satish Chandra* (1954), the Court rejected the analogy with the U.S. Fourth Amendment. Similarly, in *Kharak Singh v. State of Uttar Pradesh* (1963), the Court upheld police surveillance, with the majority refusing to recognize privacy as constitutionally protected.

(b) Progressive Developments

Later decisions cautiously opened the door. In *Gobind v. State of Madhya Pradesh* (1975), the Court hinted at privacy as part of Article 21, though subject to restrictions.In *R. Rajagopal v. State of Tamil Nadu* (1994), the Court explicitly recognized the right to prevent unauthorized publication of private life, a milestone for informational privacy. *PUCL v. Union of India* (1997) further extended privacy to communications, striking down indiscriminate telephone tapping.[1]

(c) *Puttaswamy* (2017)

The watershed moment came in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017). A nine-judge bench unanimously recognized privacy as a fundamental right under Part III of the

Constitution. The Court overruled *M.P. Sharma* and *Kharak Singh* to the extent inconsistent with this holding.

Justice Chandrachud's plurality opinion identified privacy's three dimensions: spatial, decisional, and informational. Privacy was framed as intrinsic to dignity, liberty, and autonomy, with implications across fundamental rights. Justice Kaul further linked privacy to freedom of thought and the right to control personal information.

(d) *Puttaswamy II* (Aadhaar Case, 2018)

The subsequent Aadhaar case tested the scope of privacy. The Court upheld Aadhaar's validity for welfare delivery but struck down provisions mandating private sector use. While the majority emphasized proportionality, Justice Chandrachud's dissent highlighted risks of surveillance and inadequate safeguards, foreshadowing contemporary critiques of India's data protection regime.

Puttaswamy's significance extends beyond India's borders. A case comment published in the American Journal of International Law observed that the six separate opinions were notable for their extensive engagement with foreign law spanning multiple jurisdictions and legal traditions, reflecting a deliberate effort to situate India's privacy jurisprudence within a global comparative tradition. This comparative methodology has itself become a subject of academic debate, with some scholars questioning how selectively courts invoke foreign precedent to support conclusions already reached on domestic grounds.[53]

(e) Privacy and Identity

Privacy jurisprudence has also informed rights relating to sexuality and identity. In *Navtej Singh Johar v. Union of India* (2018), the Court decriminalized consensual same-sex relations, grounding its reasoning in privacy, dignity, and autonomy. Similarly, in *Joseph Shine v. Union of India* (2019), adultery was decriminalized on privacy and equality grounds. These decisions demonstrate the transformative potential of privacy in expanding substantive freedoms.

2. United States: Fragmented but Influential

The U.S. judiciary has played a pioneering role, albeit inconsistently, in recognizing privacy rights.

(a) Decisional Autonomy

Griswold v. Connecticut (1965) recognized marital privacy in contraceptive choices, deriving it from the "penumbras" of constitutional guarantees. This reasoning extended in *Roe v. Wade* (1973) to abortion rights. However, *Dobbs v. Jackson Women's Health Organization* (2022)

[53] Case Comment, 'Justice K.S. Puttaswamy (Ret'd) and Anr v Union of India and Ors' American Journal of International Law (Cambridge University Press) <https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/justice-ks-puttaswamy-retd-and-anr-v-union-of-india-and-ors/ED631B8F922039BEC5400086C8E34338> accessed 26 July 2026.

overturned *Roe*, curtailing privacy-based autonomy. This reversal underscores the vulnerability of implied privacy rights in the absence of explicit constitutional guarantees.

(b) Surveillance and Digital Privacy

The Fourth Amendment has been central to privacy in surveillance contexts. In *Katz v. United States* (1967), the Court shifted focus from property to a "reasonable expectation of privacy." *United States v. Jones* (2012) applied this doctrine to GPS tracking, requiring warrants for prolonged monitoring. In *Carpenter v. United States* (2018), the Court held that warrantless acquisition of cell-site location data violated the Fourth Amendment, signalling adaptation to the digital age.

(c) Informational Privacy

The Court has been more cautious on informational privacy. In *Whalen v. Roe* (1977), it upheld a state's collection of medical data but acknowledged a constitutional interest in avoiding disclosure. While not fully developed, this recognition laid groundwork for subsequent debates.

3. Europe: Robust Judicial Protections

The European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) have developed some of the strongest privacy protections globally.

(a) European Court of Human Rights

In *Klass v. Germany* (1978), the ECtHR recognized that secret surveillance could be compatible with Article 8 but required safeguards against abuse. In *S. & Marper v. United Kingdom* (2008), the Court found that indefinite retention of DNA data violated privacy. *Big Brother Watch v. United Kingdom* (2021) further strengthened oversight of bulk interception regimes.

(b) Court of Justice of the European Union

The CJEU has expanded informational privacy through landmark decisions. In *Digital Rights Ireland* (2014), it struck down the EU Data Retention Directive for violating proportionality and privacy rights.[1] In *Google Spain SL v. AEPD* (2014), it recognized the "right to be forgotten," requiring search engines to delist personal information.

The *Schrems* cases transformed transatlantic data flows. *Schrems I* (2015) invalidated the Safe Harbor framework due to inadequate safeguards against U.S. surveillance. *Schrems II* (2020) struck down the Privacy Shield for similar reasons, underscoring the primacy of privacy in cross-border transfers.[54]

---

[54] *Data Protection Comm'r v. Facebook Ireland & Schrems (Schrems II)*, Case C-311/18, ECLI:EU:C:2020:559.

4. Inter-American and African Jurisprudence

In the Inter-American system, the Inter-American Court of Human Rights' **Advisory Opinion OC-23/17** explicitly recognized the right to data protection as part of Article 11 of the ACHR. The Court emphasized informational self-determination and transparency in digital governance.

In Africa, while the African Charter does not explicitly recognize privacy, domestic courts have begun interpreting dignity provisions expansively. For example, the High Court of Kenya in *Coalition for Reform and Democracy v. Attorney General* (2015) struck down sections of the Security Laws Amendment Act for enabling surveillance without safeguards.[1] This reflects a growing recognition of privacy in African constitutional practice.

5. Comparative Lessons

Judicial developments across jurisdictions reveal several patterns:

1. **Transformative potential**: Courts often expand privacy beyond narrow textual guarantees, linking it to dignity, autonomy, and equality.
2. **Vulnerability of implied rights**: U.S. jurisprudence demonstrates that privacy without explicit textual grounding remains fragile.
3. **Proportionality as a standard**: Both Indian and European courts emphasize proportionality in balancing privacy with state interests.
4. **Global influence of European standards**: The ECtHR and CJEU have shaped global privacy law, particularly through the GDPR and data transfer jurisprudence.
5. **Convergence on informational privacy**: Courts increasingly recognize data protection as central to privacy, though with varying institutional mechanisms.

Policy and Legislative Frameworks: National and Global

The recognition of privacy as a constitutional right must be matched by statutory frameworks that operationalize protections in practice. Legislative regimes serve to define rights, impose obligations, and establish enforcement mechanisms. A comparative survey reveals significant diversity in national and regional approaches, ranging from the European Union's comprehensive model to the United States' sectoral approach, and India's recent but evolving statutory architecture.

1. India: The Digital Personal Data Protection Act, 2023

India's journey towards a data protection framework has been shaped by the *Puttaswamy* decision (2017), which mandated legislative action to safeguard informational privacy. The government established the Justice B.N. Srikrishna Committee, whose 2018 report laid the

groundwork for a comprehensive data protection law.[55] After several iterations, Parliament enacted the **Digital Personal Data Protection Act, 2023 (DPDPA)**.

The DPDPA applies to digital personal data processed in India and to extraterritorial processing related to goods or services offered in India. It enshrines principles of legality, purpose limitation, data minimization, accuracy, and accountability. Consent is the primary basis for processing, though the Act allows processing without consent for state functions, emergencies, employment, and "legitimate uses."

Key rights under the Act include the right to access, correction, and erasure of personal data, as well as the right to grievance redressal. The Act establishes the Data Protection Board of India as the enforcement body, empowered to impose penalties for non-compliance.

Despite these provisions, the DPDPA has drawn criticism. First, it grants broad exemptions to the government for reasons of sovereignty, security, and public order. Second, the independence of the Data Protection Board is questionable, as it remains under executive control. Third, the Act permits cross-border data transfers subject to government notification, raising concerns about adequacy and transparency.

While the DPDPA reflects an important milestone, it falls short of the comprehensive safeguards envisioned in *Puttaswamy*. Compared with global standards such as the GDPR, India's framework remains state-centric and weak on enforcement.

The framework was substantially operationalised when the Ministry of Electronics and Information Technology notified the Digital Personal Data Protection Rules, 2025 on 13 November 2025, nearly two years after the parent Act received presidential assent. The Rules prescribe a staggered compliance timeline of up to eighteen months and set out detailed procedures for consent managers, breach notification, and the digital functioning of the Data Protection Board, though the Board's institutional independence from the executive remains, as before, unaddressed.[1]

2. The United States: Sectoral and Fragmented Protections

Unlike India and the EU, the United States lacks a comprehensive federal data protection statute. Instead, it relies on a **sectoral approach**, with laws targeting specific domains.

- **Health Insurance Portability and Accountability Act (HIPAA, 1996):** Protects medical data, imposing obligations on healthcare providers and insurers.[56]
- **Gramm-Leach-Bliley Act (GLBA, 1999):** Governs financial data, requiring disclosure and safeguards by financial institutions.[1]

[55] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018)

[56] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936

- **Children's Online Privacy Protection Act (COPPA, 1998):** Restricts collection of data from children under 13.[57]

In addition, the **Federal Trade Commission (FTC)** plays a central role, enforcing privacy through its powers to prohibit "unfair or deceptive acts or practices."[1] The FTC has brought enforcement actions against tech companies for misrepresenting privacy practices or failing to secure user data.

At the state level, laws such as the **California Consumer Privacy Act (CCPA, 2018)** and its successor, the California Privacy Rights Act (CPRA, 2020), have introduced GDPR-style rights, including access, deletion, and opt-out provisions.[58] Other states, including Virginia and Colorado, have followed suit.

The absence of a unified federal framework, however, creates fragmentation and inconsistency. The sectoral model leaves gaps, particularly in areas like AI, biometrics, and cross-sectoral data processing. The U.S. approach prioritizes innovation and economic growth, often at the expense of uniform privacy protections.

3. The European Union: The General Data Protection Regulation (GDPR)

The **GDPR**, adopted in 2016 and effective since 2018, represents the most comprehensive data protection framework globally.[1] It applies to all processing of personal data by entities established in the EU, as well as to non-EU entities offering goods or services to EU residents.

The GDPR is built on foundational principles: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability. Individuals enjoy robust rights, including access, rectification, erasure, restriction of processing, portability, and objection. Importantly, the GDPR requires explicit consent and grants individuals the "right to be forgotten," as recognized in *Google Spain*.

The regulation also mandates Data Protection Impact Assessments (DPIAs) for high-risk processing, and the appointment of Data Protection Officers (DPOs) in certain entities. Cross-border data transfers are permitted only to jurisdictions deemed "adequate" or subject to standard contractual clauses.[59]

Enforcement is robust, with independent supervisory authorities in each member state and the European Data Protection Board coordinating consistency. Penalties can reach up to €20 million or 4% of annual global turnover.

The GDPR has become a global benchmark, inspiring laws in Brazil (LGPD), South Korea, South Africa, and India's DPDPA. Its extraterritorial reach has reshaped corporate practices

[57] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506
[58] California Consumer Privacy Act of 2018, Cal. Civ. Code 1798.100–.199
[59] GDPR, supra note 13, arts. 44–49

worldwide, making compliance with EU standards a de facto requirement for multinational companies.

4. Regional and Global Developments

(a) Latin America

Latin American countries have increasingly adopted GDPR-inspired laws. Brazil's **Lei Geral de Proteção de Dados (LGPD, 2018)** mirrors GDPR principles, establishing consent-based processing, data subject rights, and an independent authority. Mexico, Argentina, and Chile have also enacted comprehensive frameworks, aligning with EU adequacy standards.

(b) Africa

The **African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, 2014)** sets out regional obligations, though this assessment requires updating: the Convention reached the fifteen ratifications required for entry into force when Mauritania ratified it in May 2023, and it formally entered into force on 8 June 2023, nearly a decade after its adoption. It remains, however, the only binding continent-wide data protection treaty outside Europe, and several of its fifteen ratifying states have yet to enact the domestic legislation the Convention requires.[1] South Africa's **Protection of Personal Information Act (POPIA, 2013)** provides comprehensive protections, balancing privacy with economic interests.[60]

(c) Asia-Pacific

The Asia-Pacific Economic Cooperation (APEC) Privacy Framework adopts a more flexible, principles-based approach, emphasizing accountability and cross-border interoperability rather than binding rights.[1] Japan, South Korea, and Singapore have enacted strong data protection laws, with Japan achieving EU adequacy status.[61]

5. Comparative Reflections

The comparative survey highlights key differences:

- **Scope:** The EU's GDPR is comprehensive and uniform, while the U.S. remains fragmented. India falls in between, with a broad statute but weak institutional enforcement.
- **Rights:** The GDPR provides the strongest individual rights, including portability and erasure. India's DPDPA grants limited rights, while the U.S. framework varies by sector and state.

[60] Protection of Personal Information Act 4 of 2013 (S. Afr.)

[61] European Commission, *Adequacy Decision for Japan under the GDPR* (2019)

- **Enforcement:** Independent regulators are central to the EU model. India's Data Protection Board lacks independence, and U.S. enforcement is largely reactive through the FTC.
- **Cross-Border Transfers:** The EU's adequacy model sets a high bar, influencing global practices. India's approach remains discretionary, while the U.S. relies on contractual mechanisms.
- **Balance with State Interests:** India and the U.S. prioritize state security and innovation, respectively, whereas the EU emphasizes individual rights.

6. Global Gaps and the Need for Harmonization

The divergence among frameworks creates challenges for cross-border data governance. Multinational companies face conflicting obligations, while individuals encounter uneven protections. Efforts at harmonization through forums like the OECD, APEC, and WTO remain limited.

Given the global nature of digital technologies, a coherent international framework is essential. Proposals for a binding UN convention on data protection have gained traction, but consensus remains elusive. In the meantime, the GDPR continues to serve as a "gold standard," influencing domestic laws and international negotiations.

Critical Analysis: Balancing Technology, Privacy, and Governance

The recognition of privacy as a constitutional and human right has brought about important normative and legal transformations. Yet the effective realization of privacy and data protection remains contested. Both constitutional courts and legislatures grapple with balancing competing values: individual dignity and autonomy on the one hand, and technological innovation, state security, and economic growth on the other. This section critically analyzes these tensions and offers a framework for reconciling them.

1. Privacy versus State Security

One of the most enduring tensions lies in the relationship between privacy and national security. Governments argue that surveillance is necessary to prevent terrorism, crime, and cyber threats. The Indian government has frequently invoked sovereignty and public order to justify broad exemptions under the Digital Personal Data Protection Act (DPDPA). Similarly, the United States' PATRIOT Act expanded state surveillance powers post-9/11, with significant implications for privacy.[1]

However, unchecked surveillance undermines constitutional rights. The Snowden revelations exposed the U.S. National Security Agency's mass surveillance programs, raising questions about compatibility with Article 17 of the ICCPR and the Fourth Amendment.[62] In India, critics

[62] Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* 15–19 (2014)

warn that the DPDPA's exemptions enable pervasive monitoring, contrary to the proportionality standard established in *Puttaswamy*.

The challenge is to ensure that surveillance is targeted, proportionate, and subject to independent oversight. Judicial doctrines of proportionality, as developed in India and Europe, provide useful frameworks for balancing these competing interests.

2. Privacy versus Innovation and Economic Growth

Privacy regulation often clashes with innovation and market efficiency. Tech companies argue that data is the "oil of the digital economy," and overregulation could stifle innovation.[1] The GDPR has been criticized for imposing high compliance costs, particularly on small and medium enterprises.[63]

On the other hand, weak regulation creates risks of exploitation and monopolization. The dominance of surveillance-based business models by companies such as Google, Meta, and Amazon exemplifies how unregulated data collection consolidates economic power. Such practices not only undermine individual autonomy but also distort market competition.

India's DPDPA reflects this dilemma. While it introduces principles of consent and accountability, it also grants wide latitude for state and corporate data processing, prioritizing growth and governance efficiency. A stronger emphasis on user-centric design and privacy-by-default could reconcile innovation with rights protection.

3. Privacy as an Individual and Collective Right

Traditional legal frameworks treat privacy as an individual right, exercised through consent and control. However, in the digital age, privacy has collective dimensions. Data about one individual often reveals information about others, such as genetic data or social network connections. The collection of metadata en masse affects entire communities, influencing democratic processes and public discourse.

The Cambridge Analytica scandal illustrates this collective dimension: the misuse of data from Facebook not only affected individual users but also shaped electoral outcomes.[1] Scholars argue that privacy must be reconceptualized as a public good, essential for democracy, equality, and social justice.[10]

Constitutional jurisprudence in India and Europe increasingly recognizes these broader dimensions. *Puttaswamy* linked privacy to democracy and the rule of law, while the CJEU in *Schrems II* emphasized that data protection safeguards are essential for protecting fundamental freedoms.[11]

4. Consent, Autonomy, and Power Asymmetry

---

[63] European Commission, *Impact Assessment on the General Data Protection Regulation* (2012)

Consent remains the cornerstone of most privacy frameworks. However, the reality of pervasive tracking, complex privacy policies, and power asymmetry between corporations and users renders consent largely illusory. "Notice-and-consent" models fail to capture the systemic nature of data exploitation.[64]

For example, users rarely read or understand lengthy privacy policies, and withdrawal of consent is often impractical. Behavioral advertising operates on defaults that assume consent, undermining autonomy.

Empirical research bears out the scale of this problem: a widely cited study estimated that if internet users actually read every privacy policy they encountered in a given year, the aggregate opportunity cost in lost time would approach $781 billion annually in the United States alone, at an average of roughly ten minutes per policy. Such findings suggest that "notice-and-consent" functions more as a legal formality than as a genuine exercise of informed choice.[1]

The GDPR attempts to address this by mandating clear, informed, and freely given consent, but enforcement challenges persist. India's DPDPA also emphasizes consent but weakens it by allowing broad "legitimate uses" and government exemptions. Without structural safeguards such as privacy by design, consent cannot adequately protect users.

5. Institutional Capacity and Enforcement

Even the strongest legal frameworks falter without effective enforcement. Independent data protection authorities (DPAs) are essential for oversight. The EU model of supervisory authorities and the European Data Protection Board exemplifies institutional robustness. In contrast, India's Data Protection Board lacks independence and transparency, raising concerns about capture by the executive.

The U.S. FTC, while active in enforcement, is constrained by its consumer protection mandate and limited jurisdiction. State-level authorities under laws like the CCPA offer some remedies but contribute to fragmentation.[65]

Effective governance requires not only independent regulators but also judicial engagement and civil society participation. Courts must interpret statutory frameworks in light of constitutional guarantees, ensuring proportionality and accountability.

6. Global Fragmentation and Extraterritoriality

Divergent frameworks create challenges for cross-border governance. The EU's GDPR asserts extraterritorial reach, applying to companies outside the EU that process data of EU residents. While this strengthens protections, it also creates compliance burdens and jurisdictional conflicts.[1]

---

[64] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880, 1882–83 (2013)

[65] Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583, 612–14 (2014)

India's discretionary approach to cross-border transfers reflects concerns about data sovereignty but lacks transparency.[66] This gap has since narrowed on paper, if not entirely in practice. The Digital Personal Data Protection Rules, 2025 permit the Central Government to restrict the transfer of specified categories of personal data outside India on the recommendation of a dedicated committee, but the categories of data subject to such restrictions, and the criteria the committee will apply, had yet to be publicly specified as of the Rules' notification.[1] The U.S. relies heavily on contractual mechanisms, leaving protection uneven. The absence of a global treaty exacerbates fragmentation, undermining trust in digital commerce and human rights protections.

Efforts such as Convention 108+ and APEC's Cross-Border Privacy Rules (CBPR) system represent steps toward harmonization but remain regionally limited.[67] A binding UN convention on digital rights, including privacy, has been proposed but faces geopolitical resistance.

7. The Proportionality Principle as a Unifying Framework

Across jurisdictions, proportionality analysis has emerged as a key doctrinal tool. Courts in India, Europe, and Latin America apply proportionality to balance privacy with competing interests. The test typically involves four prongs: legality, legitimacy, necessity, and proportionality in the strict sense.

For example, in *Puttaswamy*, the Indian Supreme Court applied proportionality to evaluate Aadhaar.[22] Similarly, the CJEU in *Digital Rights Ireland* and *Schrems II* used proportionality to strike down overbroad surveillance and data transfer regimes.[23]

Proportionality offers a structured method for reconciling technological innovation, state interests, and individual rights. However, its effectiveness depends on rigorous application and institutional independence.

8. Normative Recommendations

A critical analysis of privacy governance suggests several reforms:

1. **Strengthening independence of regulators:** Data protection boards and authorities must be insulated from executive influence.
2. **Enhancing user agency:** Privacy by design, default protections, and collective rights frameworks can reduce reliance on weak consent models.

[66] Government of India, Draft National E-Commerce Policy (2019)

[67] Council of Europe, Convention 108+, Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data (2018).

3. **Embedding accountability in technology:** Algorithmic transparency, impact assessments, and liability frameworks should be mandated.
4. **Balancing sovereignty and flows:** Cross-border data governance should prioritize interoperability rather than strict localization.
5. **Advancing international cooperation:** Multilateral agreements on privacy and cybersecurity should be pursued under the UN or WTO frameworks.

The challenge of balancing technology, privacy, and governance is both normative and institutional. While courts and legislatures have advanced privacy protections, gaps persist due to weak enforcement, power asymmetries, and global fragmentation. Reconceptualizing privacy as both an individual right and a collective good offers a way forward. By embedding proportionality, accountability, and user-centric design into legal and technological systems, constitutional and international frameworks can adapt to the demands of the digital age.

Recommendations and Conclusion

1. Key Insights from the Study

This paper has traced the evolution of privacy and data protection from its early conception as a spatial right to its modern articulation as a multidimensional entitlement encompassing autonomy, dignity, and informational self-determination. Constitutional jurisprudence in India, particularly the *Puttaswamy* case, has brought privacy to the forefront, while international standards such as the ICCPR and GDPR have institutionalized global commitments. However, technological transformations—AI, biometrics, surveillance capitalism, and cross-border flows—continue to challenge traditional frameworks.

Comparative analysis reveals a spectrum of approaches: the EU's comprehensive and rights-centric GDPR; the U.S.'s fragmented, sectoral regime; the U.K.'s hybrid model integrating ECHR standards; and India's nascent but evolving Digital Personal Data Protection Act (2023). Judicial decisions across jurisdictions underscore the centrality of proportionality, accountability, and transparency, but enforcement remains uneven.

The critical analysis demonstrates that privacy cannot be adequately protected through individual consent alone; it must also be framed as a collective right and structural principle essential for democracy and human dignity.

2. Recommendations for National Frameworks

(a) India

1. **Strengthening the Independence of the Data Protection Board:** The Board must be institutionally insulated from executive control to ensure impartial oversight.

2. **Narrowing Government Exemptions:** The DPDPA's broad carve-outs for sovereignty, public order, and security should be narrowed through precise statutory definitions and subject to judicial review.

3. **Enhancing User Rights:** India should expand user rights to include portability and the right to be forgotten, aligning with GDPR standards.

4. **Incorporating Privacy by Design:** Mandating technical and organizational safeguards such as default data minimization can reduce reliance on consent.

5. **Capacity Building:** Investments in digital literacy and awareness campaigns are essential to enable meaningful exercise of privacy rights.

(b) United States

1. **Adopting a Comprehensive Federal Privacy Law:** The U.S. should move beyond its fragmented sectoral approach to a unified federal statute, harmonizing protections across domains.

2. **Strengthening FTC Powers:** The FTC requires expanded authority and resources to regulate digital platforms effectively.

3. **Ensuring Algorithmic Transparency:** Statutory frameworks should mandate disclosures and impact assessments for high-risk AI systems.

(c) European Union

The EU has already set high standards, but refinements are necessary:

1. **Balancing Compliance Costs:** Support mechanisms for SMEs could mitigate the disproportionate burden of GDPR compliance.

2. **Clarifying Automated Decision-Making Rules:** Ambiguities in Article 22 of the GDPR regarding profiling should be clarified to ensure enforceability.

3. **Cooperation with Third States:** Enhanced mechanisms for global adequacy partnerships could reduce fragmentation and foster convergence.

3. Recommendations for International Governance

The global nature of data flows demands cooperative solutions.

1. **Toward a Binding UN Convention on Digital Rights:** Building on the UDHR and ICCPR, the UN could negotiate a convention specifically addressing digital privacy, AI, and cross-border data governance.

2. **Interoperability of Regional Frameworks:** Initiatives such as APEC's Cross-Border Privacy Rules (CBPR) and Council of Europe's Convention 108+ should be harmonized to reduce regulatory fragmentation.

3. **Embedding Privacy in Trade Agreements:** Future WTO negotiations and bilateral trade agreements should integrate binding privacy clauses to ensure that data flows respect human rights.

4. **Global Oversight Mechanisms:** Establishing an international data protection authority or multilateral review body could enhance accountability for surveillance practices.

4. Addressing Emerging Technologies

Regulation must anticipate emerging threats rather than react to them.

- **Artificial Intelligence:** States should require algorithmic audits, bias testing, and transparency measures for AI systems. The EU's Artificial Intelligence Act, which entered into force on 1 August 2024, offers a useful model. The Act, formally Regulation (EU) 2024/1689, introduces a risk-tiered framework that bans certain unacceptable-risk applications outright and imposes graduated obligations, including conformity assessments and human oversight, on high-risk systems. States such as India, which currently regulate artificial intelligence only through non-binding guidelines, could draw on this tiered approach when designing statutory safeguards.[1]
- **Biometrics:** Global standards on biometric data collection and retention are urgently needed to prevent misuse.
- **Genetic and Health Data:** Robust consent and anonymization requirements must protect genetic information, given its familial and intergenerational implications.
- **Quantum Computing:** International cooperation on encryption standards is necessary to preempt risks from quantum decryption capabilities.

5. Reconceptualizing Privacy as a Collective Good

The paper argues that privacy must be reframed not only as an individual right but as a public good. Mass surveillance, data monopolies, and AI profiling affect entire communities and democratic institutions. This collective dimension requires structural protections that go beyond individual consent. Courts and legislatures should increasingly treat privacy as a prerequisite for equality, democracy, and social justice.

6. Conclusion

The intersection of technology, privacy, and data protection embodies one of the defining challenges of constitutional and international law in the 21st century. While India's recognition of privacy in *Puttaswamy* was a landmark, the country's statutory framework remains incomplete. Globally, the GDPR sets the gold standard, but fragmentation persists due to divergent national models and geopolitical tensions.

Judicial developments reveal that privacy is a living right, constantly reinterpreted in light of new technologies. Yet courts alone cannot ensure effective protection. Legislative frameworks,

independent regulators, international cooperation, and technological safeguards are equally indispensable.

The future of privacy governance requires a recalibration of priorities: innovation and security must be pursued within the bounds of proportionality, accountability, and human dignity. International harmonization, coupled with strong national frameworks, can create a rights-respecting digital ecosystem. Ultimately, privacy in the digital age is not merely about protecting individuals from intrusion—it is about safeguarding the foundations of liberty, equality, and democracy in an interconnected world.