Right to Privacy in the Digital Age

Sengar S.P.[1], Abraham S.[2]

[1]5th Year, BALLB (Hons), Hindustan Institute of Technology and Science, Chennai

[2]Assistant Professor, Hindustan Institute of Technology and Science, Chennai

***Abstract*—The digital revolution has dramatically transformed the scope and challenges of the right to privacy. International human rights law (e.g. UDHR Art. 12, ICCPR Art. 17) has long recognized privacy as fundamental, but recent technologies have exposed limits in existing frameworks. Data-intensive tools—from smartphones to AI—now allow unprecedented surveillance and data profiling. This paper examines how legal systems worldwide are adapting: it reviews international standards, regional laws (EU, US, India, etc.), and case law (e.g. Riley, Carpenter, Google Spain) that define digital privacy rights. The literature highlights a global wave of new privacy legislation and calls for flexible, rights-preserving regimes. Our analysis uses doctrinal and comparative methods to assess statutory protections, judicial rulings, and policy debates. We find that while landmark decisions have extended privacy protections to personal data and communications, significant threats remain (mass surveillance, spyware, AI). The paper concludes by suggesting stronger safeguards: robust data protection enforcement, transparency of surveillance practices, privacy-by-design in technology, and international cooperation to uphold privacy in an increasingly networked world.**

***Keywords*—Privacy; Digital rights; Data protection; Surveillance; GDPR; Fundamental rights**

I. Introduction

Privacy has long been recognized as a fundamental human right. International instruments enshrine the right to privacy, including Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). However, the emergence of the Internet, social media, smartphones, and the 'Internet of Things' has exponentially increased personal data collection and processing. Modern digital technologies enable governments and corporations to track, analyze, and even manipulate individuals' behavior on an unprecedented scale. UN reports warn that these developments pose 'very significant risks for human dignity, autonomy and privacy' unless effective safeguards are in place. Scholars note that traditional privacy laws—designed for a pre-digital era—often lag behind rapid innovation. Nasir (2025) observes that data harvesting across digital media has swept through privacy laws globally, raising legal and ethical questions about personal data protection.

In sum, the digital age has transformed privacy into a contested field: it is more vulnerable to abuse (through mass surveillance, big data profiling, spyware, etc.) while also being reinforced by new rights-based regulations (GDPR, privacy by design, etc.). This study explores how the right to privacy is evolving in this context. The paper surveys recent literature and legal developments. It first reviews scholarly and policy analyses of privacy in the digital age. Next, it examines the legal framework: international human rights guarantees, regional statutes like the EU's GDPR, case law in the United States and India, and emerging laws worldwide. We highlight landmark judgments (e.g. Riley v. California and Carpenter v. U.S.) that expanded privacy protections to personal devices and data. Finally, we analyze current challenges—mass surveillance, state security laws, data breaches, AI-driven profiling—and propose recommendations for balancing privacy with other interests.

II. Review of Literature

The scholarly literature on privacy in the digital age emphasizes that rapid technological changes have outpaced legal protections. Authors note that the 'revolution of the digital era' has forced a shift in how

privacy is conceived and protected. Historically, privacy was concerned with physical spaces and personal communications; now it encompasses online activities, metadata, and complex data flows. Researchers argue that many existing laws are reactive rather than proactive, prompting calls for flexible legal frameworks that can adapt without sacrificing individual rights. For example, Nasir (2025) describes how global responses like the EU's GDPR and California's CCPA represent milestones in privacy legislation, yet acknowledges ongoing debates over consent models, data transparency, and breaches.

Academic and policy analyses also focus on tensions between privacy and other values. Privacy International observes that unchecked mass surveillance (through CCTV, internet monitoring, and data retention) fundamentally threatens democratic freedoms. Reports by the UN and ACLU highlight how new surveillance technologies (spyware, facial recognition, AI analytics) can disproportionately harm marginalized groups and chill speech. Several authors document the concept of the 'right to be forgotten' stemming from Google Spain and its critics: while some see it as essential for personal dignity, others warn it may conflict with free expression rights. Empirical surveys even find broad public support for more control over online data.

Comparative studies reinforce that legal approaches vary. European scholars often note the GDPR's comprehensive scope and emphasis on user consent and data minimization, whereas U.S. commentators point to a fragmented, sectoral regime and constitutional limits on government intrusion. In India, legal scholarship after Puttaswamy (2017) has debated how to balance privacy against transparency (RTI) and security. Trends literature (e.g. Gibson Dunn 2024) shows a clear global trend: by 2023, new data protection laws were being enacted worldwide (in India, Vietnam, Saudi Arabia, etc.), reflecting both legislative momentum and policy learning across borders. Overall, the literature underscores gaps: many critics lament uneven enforcement of privacy rights and call for stronger international cooperation to protect privacy across jurisdictions.

III. Research Methodology

This study employs qualitative legal research methods. It is doctrinal and comparative in nature: we systematically review primary sources (statutes, case law, official documents) and secondary scholarship on privacy law. The approach includes statutory analysis—examining key laws such as the GDPR and Digital Personal Data Protection Act 2023 to identify privacy rights and obligations; case law analysis—analyzing landmark judicial decisions (Riley v. California, Carpenter v. United States, Puttaswamy v. Union of India) to understand how courts interpret privacy in the digital context; literature review—synthesizing academic articles, NGO reports, and policy papers from the UN, ACLU, and privacy NGOs to capture prevailing analyses and critiques; and a comparative perspective—contrasting different legal systems (EU, US, India, others) to reveal common principles and divergent approaches.

No empirical data collection was involved; instead, the methodology is interpretive. By integrating doctrinal analysis with theoretical insights, we aim to provide a comprehensive account of how the right to privacy is conceptualized and implemented in the digital age.

IV. International and Regional Frameworks

International Human Rights Law

At the global level, privacy is firmly recognized. Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights guarantee protection against 'arbitrary or unlawful interference' with privacy. In practice, these provisions have been interpreted to cover modern concerns, though treaty bodies have noted the need to revisit them in light of technology. For example, the UN Human Rights Committee's General Comment No. 16 (1988) on ICCPR Art. 17 was aimed at setting standards for state intrusions, and scholars argue for a new General Comment to specifically address digital threats. The UN High Commissioner for Human Rights and privacy experts have held consultations emphasizing that data-driven tools (AI, big data analytics, ubiquitous networks) must be regulated to uphold human rights norms. In short, the international framework provides a normative baseline: privacy is a fundamental right, but the details are evolving through soft law, guidelines, and domestic implementation.

European Union

The EU has the most robust formal protections. The EU Charter of Fundamental Rights (Article 7) and the ECHR (Article 8) explicitly protect private life. In legislative terms, the General Data Protection Regulation (GDPR, Reg. 2016/679) was a landmark reform. As the European Commission notes, the GDPR was 'an essential step to strengthen individuals' fundamental rights in the digital age.' It harmonized data protection across member states, mandating principles like consent, data minimization, and rights of access, erasure, and portability. Notably, GDPR has extraterritorial reach, affecting any company processing EU personal data.

EU courts have also extended privacy rights. In Google Spain v. AEPD (2014), the CJEU recognized a 'right to erasure' allowing individuals to have search engines remove links to outdated personal information. The Court held that the fundamental right to privacy can outweigh the economic interest of the search company in certain contexts. This has led to millions of takedown requests in the EU. On transatlantic data flows, following the Schrems II decision (2020) invalidating the EU–US Privacy Shield, the EU and US in 2023 agreed on a new Data Privacy Framework, instituting new safeguards including limits on intelligence access and a Data Protection Review Court.

United States

The U.S. has no single constitutional guarantee of privacy, but the Fourth Amendment and various statutes create a patchwork. The Fourth Amendment protects against unreasonable searches and seizures, and the Supreme Court has adapted it to digital contexts. In Riley v. California (2014), the Court unanimously ruled that police generally cannot search a cell phone's digital data without a warrant, because such searches intrude on 'substantially greater' privacy interests than a search of physical items. Later, in Carpenter v. United States (2018), the Court held that obtaining a week's worth of cell phone location records without a warrant violated the Fourth Amendment. These cases signal that digital data held by third parties (like phone carriers) can still be protected.

Outside the Constitution, U.S. privacy protection is sectoral (e.g. HIPAA for health data, COPPA for children's data). Notably, California enacted the CCPA (2018) for consumer data rights, and in 2023 passed the CPRA, enhancing privacy rights in that state. Critics note that U.S. law lags behind the EU: Americans rely more on corporate policy and limited regulations, whereas Europeans have a rights-based system. The U.S. debate continues over balancing privacy with national security and free expression.

India

In India, privacy has rapidly ascended as a constitutional right. The Supreme Court's K.S. Puttaswamy v. Union of India (2017) was a watershed: a nine-judge bench unanimously held that privacy is a fundamental right under Article 21 (Right to Life and Personal Liberty) of the Constitution. The Court explicitly recognized informational privacy as integral to personal liberty. Puttaswamy did not specify the content of the right or detailed safeguards; instead, it struck down a national biometric ID program (Aadhaar) for being disproportionate in lack of consent. Subsequent judgments have emphasized that privacy can be limited for legitimate public purposes, requiring a balancing test.

On the legislative front, India enacted its first comprehensive data protection law in August 2023: the Digital Personal Data Protection Act (DPDP Act, 2023). The DPDP Act establishes an economy-wide framework: it requires data fiduciaries (controllers) to obtain free, informed consent; it grants data principals (individuals) rights to access, correct, or erase personal data; and it imposes obligations on companies for data security, audits, and transparency. The law's extraterritorial scope covers processing for Indian residents. Notably, the DPDP Act introduces enforcement mechanisms including penalties up to ₹250 crore and a Data Protection Board. Experts observe the DPDP Act is 'more streamlined and focused' than prior bills, after extended deliberation. In practice, its implementation is still evolving, with draft rules circulated in 2025.

Other countries also illustrate varied approaches. Brazil's LGPD (2018) closely mirrors the GDPR. China's Personal Information Protection Law (2021) created a broad regime with strict consent and government allowances. In 2023, multiple jurisdictions including Switzerland, UK, Vietnam, and Saudi Arabia adopted or updated data privacy laws, signaling a global convergence toward formal data protection regimes. Each system reflects local values: some emphasize individual control (EU), others focus on state authority (China, India's initial proposals), and all grapple with enforcement capacity.

V. Emerging Challenges and Debates

Despite these legal developments, significant challenges persist in the digital environment. Mass Surveillance and Data Collection: Privacy watchdogs warn that governments now collect data on vast populations regardless of suspicion, a practice often termed mass surveillance. Such indiscriminate data collection—communications metadata, location, financial transactions—can 'directly threaten the very core of our right to privacy.' The use of sophisticated spyware (e.g. Pegasus) illustrates the danger: a UN report describes how such tools can convert smartphones into 24/7 surveillance devices, enabling intrusion into all aspects of life. These capabilities have been misused against journalists, activists, and dissidents, leading UN experts to call for a moratorium on hacking tools until human rights safeguards are in place. At the same time, encryption has become a key battleground: the UN report urges states not to weaken encryption, since robust encryption is 'a key enabler of privacy and human rights online.'

Big Data and AI: Data-driven algorithms pose novel threats. Machine learning on personal data can reveal sensitive insights—health, political views, etc.—without individuals' knowledge or consent. The UN High Commissioner's office cautions that AI-driven profiling can exacerbate discrimination and control, and has recommended that AI systems incompatible with human rights be banned or strictly limited. For example, facial recognition in public spaces raises concerns about constant biometric tracking. These issues go beyond traditional privacy—they implicate dignity and autonomy. The literature suggests that legal frameworks must address not only data collection but also automated decision-making, such as the GDPR's right to explanation of algorithmic decisions.

Balancing Privacy with Security and Transparency: Another debate is how privacy intersects with other public values. Governments often cite national security or public safety to justify surveillance and data retention. Many privacy laws carve out national security or law-enforcement exceptions. In India, this tension is acute: privacy (Article 21) must be weighed against the right to information (Article 19) and collective security. The Diplomat article notes concerns that the new DPDP Act's exemptions may limit transparency under India's RTI Act. Similar dilemmas exist in other countries. Courts and legislatures continue to grapple with these trade-offs, emphasizing principles of necessity and proportionality.

Private Sector and Data Economy: Commercial exploitation of personal data adds complexity. Tech companies collect vast amounts of user data for profit. Privacy advocates lament the lack of comprehensive U.S. federal law governing this, and note that even GDPR enforcement is uneven. The literature also discusses market-based 'notice and consent' regimes as insufficient. There is growing discussion of alternative models (data trusts, privacy-by-design obligations, information fiduciary principles) to address power imbalances between individuals and data controllers.

In summary, the digital age amplifies traditional privacy issues and introduces new ones such as cybersecurity of personal information and algorithmic profiling. The existing research and reports unanimously call for stronger, more adaptable legal protections. Nasir (2025) argues for 'flexible legal regimes' that evolve with technology without trading off privacy rights. These concerns shape the recommendations below.

VI. Conclusion

The analysis reveals a complex and evolving landscape of digital privacy protection. On one hand, there has been significant progress in recognizing and codifying digital privacy as a fundamental right. Courts and legislatures across jurisdictions have extended constitutional protections into the digital sphere. India's Supreme Court has affirmed informational privacy as intrinsic to constitutional liberty, the European Union's GDPR has strengthened data subject rights, and U.S. courts have applied Fourth Amendment protections to smartphones and digital data. In parallel, many governments have enacted comprehensive data protection laws or modernized existing frameworks, including India's Digital Personal Data Protection Act, 2023. These developments reflect an emerging global consensus that individuals must retain meaningful control over their personal data and that misuse of such data can constitute a violation of fundamental rights.

However, vulnerabilities persist. Rapid technological advancement, pervasive digital surveillance, opaque data harvesting by private corporations, and the increasing use of predictive analytics pose

continuous challenges to privacy protections. As emphasized by the United Nations, 'the right to privacy is more at risk than ever before.' Thus, while doctrinal recognition and statutory codification have advanced significantly, the effectiveness of digital privacy protection ultimately depends on implementation, oversight, and adaptive governance mechanisms capable of responding to evolving technological realities.

VII. Suggestions

To address the identified gaps and strengthen digital privacy protection, several policy and regulatory measures are recommended.

1. Strengthen Enforcement Mechanisms

Privacy laws must be supported by robust enforcement structures. Data Protection Authorities (DPAs) should be adequately resourced, institutionally independent, and empowered to investigate violations and impose meaningful sanctions. International cooperation among DPAs is essential to address cross-border data flows and transnational breaches. Civil society organizations and investigative media must also play an active role in ensuring accountability of both governments and private corporations.

2. Limit Surveillance and Safeguard Security Proportionately

Clear statutory limits must govern state surveillance powers. Exceptional investigative tools, including digital interception or hacking measures, should require prior judicial authorization and be narrowly tailored to address serious and demonstrable threats. Strong encryption should be preserved as a core privacy safeguard, consistent with recommendations from UN experts. Transparency regarding surveillance frameworks and periodic public reporting can further deter misuse and reinforce democratic oversight.

3. Embed Privacy by Design

Technology developers and corporations should incorporate privacy safeguards at the design stage. Data minimization, anonymization techniques, and privacy-protective default settings reduce systemic risk. Regulators can mandate privacy impact assessments for emerging technologies. The GDPR model—requiring data protection officers, transparent notices, and compliance documentation—provides a structured framework that can guide other jurisdictions.

4. Enhance Public Awareness and Digital Literacy

Legal rights are meaningful only when individuals understand and exercise them. Public education initiatives should inform citizens about privacy risks, available remedies, and digital hygiene practices. Simplified privacy notices and user-friendly mechanisms for exercising rights such as access, correction, and erasure can significantly enhance practical empowerment.

5. Ensure Continuous Balancing and Oversight

Legislative and judicial bodies must continuously balance privacy against competing legitimate interests such as national security, public health, and transparency. Oversight mechanisms should safeguard journalists, activists, and whistleblowers from disproportionate data retention or surveillance. Policymaking should recognize privacy as foundational to other democratic freedoms, including speech, protest, and dignity.

Finally, regulatory frameworks must remain flexible and adaptive. As technology evolves, so must the law. Periodic statutory review, rule-making updates (such as under India's DPDP framework), and international harmonization efforts are essential to prevent regulatory arbitrage. The future of digital privacy will depend on vigilant enforcement, institutional independence, and innovative legal responses that ensure technological advancement does not undermine individual autonomy and human dignity.

VIII. References

ACLU (American Civil Liberties Union), 2015. Privacy and Human Rights: Principles for a Modern Right to Privacy under the ICCPR. (Report, ACLU).

Burman, A., 2023. Understanding India's New Data Protection Law. Carnegie Endowment for International Peace (Oct. 3, 2023).

Carpenter v. United States, 2018. 138 S. Ct. 2206 (U.S.).

Electronic Privacy Information Center (EPIC), 2020. The Right to Be Forgotten (Google v. Spain). (EPIC website).

European Commission, 2024. Legal framework of EU data protection. European Union, Directorate-General for Justice.

Gibson, Dunn & Crutcher LLP, 2024. International Cybersecurity and Data Privacy Review and Outlook – 2024 (client alert, Feb. 16, 2024).

Hecht-Felella, L., 2021. The Fourth Amendment in the Digital Age. Brennan Center for Justice (NYU School of Law).

Nasir, K., 2025. "The Evolution of Privacy Laws in the Digital Age." International Journal of African Sustainable Development Research 7(2).

Office of the United Nations High Commissioner for Human Rights (OHCHR), 2021. OHCHR and privacy in the digital age. (UN OHCHR website).

Office of the United Nations High Commissioner for Human Rights (OHCHR), 2022. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns. (Press release, Sept. 16, 2022).

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

Siatitsa, I., 2020. Article 12: The right to privacy. Digital Freedom Fund (Dec. 10, 2020).

Upadhyay, A. & Mehrotra, A., 2025. "India: Navigating Privacy and Transparency in the Digital Age." The Diplomat (June 9, 2025).

Footnotes

[1] Article 12: The right to privacy – Digital Freedom Fund. https://digitalfreedomfund.org/digital-rights-are-human-rights/article-12-the-right-to-privacy/

[2] ACLU. https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf

[3] [24] OHCHR and privacy in the digital age | OHCHR. https://www.ohchr.org/en/privacy-in-the-digital-age

[4] [10] [22] [23] [25] Spyware and surveillance: Threats to privacy and human rights growing, UN report warns | OHCHR. https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

[5] [14] [16] [18] [19] [20] [21] International Cybersecurity and Data Privacy Review and Outlook – 2024 - Gibson Dunn. https://www.gibsondunn.com/international-cybersecurity-and-data-privacy-review-and-outlook-2024/

[6] [7] [11] Nasir, K. (2025). The Evolution of Privacy Laws in the Digital Age. https://www.researchgate.net/publication/389955318_THE_EVOLUTION_OF_PRIVACY_LAWS_IN_THE_DIGITAL_AGE

[8] Riley v. California | 573 U.S. 373 (2014) | Justia U.S. Supreme Court Center. https://supreme.justia.com/cases/federal/us/573/373/

[9] The Fourth Amendment in the Digital Age | Brennan Center for Justice. https://www.brennancenter.org/our-work/policy-solutions/fourth-amendment-digital-age

[12] Legal framework of EU data protection - European Commission. https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

[13] Understanding India's New Data Protection Law | Carnegie Endowment for International Peace. https://carnegieendowment.org/russia-eurasia/research/2023/10/understanding-indias-new-data-protection-law

[15] EPIC - The Right to Be Forgotten (Google v. Spain). https://archive.epic.org/privacy/right-to-be-forgotten/

[17] India: Navigating Privacy and Transparency in the Digital Age – The Diplomat. https://thediplomat.com/2025/06/india-navigating-privacy-and-transparency-in-the-digital-age/