Central University of Kashmir Law Review
Online First
eISSN: 2583-6935
pp. xxx-xxx

Digital Footprint Dilemma and Privacy in the Age of Big Data: A Critical Evaluation

Ashish Kumar Singhal[*]
Priya Aggarwal[ǂ]

Abstract

The fastened enhancement of digital technology has revolutionized how information is shared and accessed that triggered both unprecedented opportunities and significant challenges for the right to privacy. In the digital age, personal data has become an invaluable resource, often traded and exploited by digital platforms, governments, and corporations. This paper is segmented into three parts. The opening segment explores the evolving concept of privacy in the digital age in the presence of the challenges posed by data collection, surveillance, and the widespread use of digital platforms in conjunction with World Wide Cyber Crime Victim Statistics and also analyses the recent data breach cases. The second part assesses the legal frameworks governing privacy rights having a focus on the effectiveness of regulations in the UK, the US, and India. The third and final section provides a series of recommendations for strengthening privacy protections, addressing gaps in existing laws, and proposing solutions for adapting to emerging technological trends.

Keywords: *Privacy, Technology, Fundamental Right, Digital Era, Data Protection, Legal Recognition*

1. Introduction

> Privacy is not Something that I'm merely Entitled to, It's an Absolute Prerequisite
>
> - Marlon Brando

Privacy is an intrinsic facet of human dignity, autonomy, and freedom that enabled individuals to preserve command over their personal information, thoughts inclusive of actions and decide how it is shared and used. With the emergence of technology, the infringement of privacy has become a significant concern. The 21st century has

[*] Associate Professor, The ICFAI University, Dehradun, Uttarakhand, India. email: ashish.singhal@iudehradun.edu.in
[ǂ] LLM Student, The ICFAI University, Dehradun, Uttarakhand, India

introduced a variety of tools and platforms that can gather, stockpile as well analyse enormous volumes of personal data. Social media platforms, mobile applications, and other connected devices constantly accumulate information about users, often without their explicit consent or understanding. This data can be used for targeted advertising, surveillance, and even manipulation, raising ethical and legal questions. Unintended privacy breaches in the virtual world are increasingly common as cyberspace blurs the lines between public and private, with personal information shared on platforms often stored indefinitely and exposed to global audiences. Mobile apps exacerbate this issue by collecting excessive data without clear consent, using weak security, sharing data with third parties, and retaining information even after deletion, heightening privacy risks. The dark web, a hidden segment of the internet, further complicates privacy concerns, as it offers anonymity but also serves as a haven for illicit activities, underscoring the need for stronger privacy protections and regulations across all digital platforms. Unlike in the pre-digital era, where people had more control over the information they shared, as digital platforms become more embedded in ordinary living, much of the data is collected passively, third-party entities and corporations possess sophisticated technologies capable of monitoring communications, browsing habits, GPS locations, social media activity, and even biometric data and analysing behaviour patterns. Although these technologies enhance security and convenience, raising significant questions about the adequacy of existing privacy protection. The term 'Privacy" was earliest systematically articulated and defined by American legal scholars Samuel D. Warren and Louis D. Brandeis. They argued that advancements in technology and the rise of the media were progressively obstructed upon individuals' private lives, necessitating legal protection against such invasions. The article emphasized the need to safeguard the "right to be let alone," which they described as an individual's right to control their personal information and preserve their dignity from unjustified public exposure. This work placed the groundwork for modern privacy law, influencing the development of legal principles that continue to shape privacy rights today.[1]

[1] Warren and Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. IV, Dec 15, 1890, No. 5.

2. Research Objectives

a) To explore the impact of digital technologies on individual's privacy.
b) To analyse the effectiveness of existing privacy laws and regulations.
c) To conduct a comparative study of laws of developed countries like the US and the UK.
d) To propose recommendations for strengthening privacy protections in response to emerging technological trends.

3. Research Questions

This paper aims to answer the following key research questions:

a) How has the digital revolution reshaped the collection, analysis, and utilization of personal data, and what implications does this have for individual privacy?
b) What role do regulatory frameworks play in ensuring data protection, and how effective are they in different countries?
c) What legal, technological, and ethical reforms are necessary to strengthen privacy rights and protections in the 21st century?
d) Should India consider adopting measures used by developed countries like the USA, UK, to address the issue of online data privacy?

4. Methodology

This research paper employs a multi-facet approach and data is collected from various journals, articles, case laws, official websites of government and research papers available on online platforms. Comprehensive analysis was conducted to study variations in constitutional provisions across different countries.

5. Literature Review

A comprehensive literature review was conducted to gather existing knowledge on the topic, the review covered academic articles, legal cases, legislative documents, and reports from international privacy organizations. This review provided a foundation for understanding the current state of privacy and identifying gaps in existing research.

(a) Warren and Brandeis[2] **(1890):** The article "The Right to Privacy," authored by Samuel D. Warren and Louis D. Brandeis, was published in the Harvard Law Review on December 15, 1890. It is widely regarded as a radical work in the development of privacy law in the United States. In this article, Warren and Brandeis argue that the instantaneous advancements in technology and the rise of mass media, particularly newspapers and photography, necessitate the recognition of a new legal right: the right to privacy. They contend that existing legal frameworks, such as defamation and intellectual property law, were insufficient to protect individuals from unwanted intrusions into their personal lives. The authors propose that privacy should be understood as "the right to be let alone," highlighting that individuals have a right to control the publication of intimate or private information about themselves. They support their argument with an analysis of common law principles while suggesting that the protection of private life could be inferred from existing legal doctrines, such as those governing property rights, contracts, and torts. It advocates for the expansion of legal protections to cover non-physical intrusions, such as the unauthorized publication of private facts and it sets the stage for the future development of privacy rights in the U.S. legal system. Their work had a remarkable influence on privacy law and continues to be cited in modern legal discussions about personal autonomy and the balance between free speech and individual privacy.

(b) Helen Nissenbaum[3] **(2009):** In her influential work on digital privacy, she argues that privacy concerns arise not from sharing information but from its inappropriate distribution. She challenges the prominence on individual control over personal data and suggested instead that privacy norms should be context-specific, fluctuating by social settings like workplaces or healthcare. Nissenbaum criticizes simplistic public-private distinctions in privacy policies, contending they often obscure crucial issues. She warns that information systems that ignore social norms can erode trust and damage the social fabric including the need for context-driven privacy protections to uphold individual dignity in the digital age.

---

[2] Ibid.

[3] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life,* Nov 24, 2009

(c) Naavi[4] **(2020):** This book by Naavi provides an in-depth analysis of India's Personal Data Protection Act (PDPA) of 2020, targets at raising awareness about the evolving data privacy landscape. The author delves into the importance of being prepared and compliant with the upcoming legal frameworks designed to protect personal data in India. It discusses the obligations that businesses and organizations must fulfil to ensure compliance with PDPA, as well as the rights granted to individuals under this law. The book draws attention on how companies must adopt data protection measures to avoid hefty penalties and legal liabilities. Through practical guidance, it explains key provisions of the PDPA, such as the lawful processing of personal data, the role of Data Protection Officers (DPOs), data localization requirements, and measures for obtaining consent from individuals. Additionally, the book presents the global context of privacy laws and how India's PDPA fits within the broader international regulatory landscape, offering comparisons with GDPR (General Data Protection Regulation) and other frameworks. Naavi's guide serves as a comprehensive resource for data protection professionals, organizations, and individuals, encouraging proactive measures to ensure compliance while safeguarding personal information in the cyber era.

(d) CA Shagun Kabra and Ms. Khyati Lad[5] **(2023):** Scholarly works have explored the trade-offs between technological advancements and individual privacy that underlined the need for legal frameworks to protect personal data. The article under review examines this issue in the light of India's Digital Personal Data Protection Act (DPDP Act) which work towards to address the rising threat to privacy brought on by technological developments.

(e) Centre for Information Policy Leadership[6] **(2024):** The increasingly complexity of privacy laws across U.S. states coupled with the absence of a uniform federal standard poses considerable compliance challenges for organizations managing personal data.

---

[4] Naavi, "*Personal Data Protection Act of India (PDPA 2020): Be Aware, Be Ready and Be Compliant"*, Notion Press, Feb 12, 2020.

[5] CA Shagun Kabra and Ms. Khyati Lad, Advancement Of Technology, Lack Of Privacy: Pre-Requisite Of The Digital Personal Data Protection Act, 2023., Volume 11, *IJRAR,* 52, 49-57, 2023.

[6] Comparison of US State Privacy Laws: Data Protection Assessments, Centre for Information Policy Leadership ("CIPL"), Feb 8, 2024.

The Centre for Information Policy Leadership (CIPL) has responded by producing a series of papers outlining these issues and offering policy recommendations to harmonize regulatory approaches.

6.1 Unintended Privacy Breaches in the Virtual World

Cyberspace plays a pivotal role in shaping the modern understanding of privacy, cyberspace refers to the virtual environment of the internet, where people interact, share information, and conduct activities like communication, commerce, and entertainment through mobile apps. Cyberspace or virtual world blurs the boundaries between public and private spheres. Social media platforms encourage individuals to share personal details, sometimes leading to unintended privacy breaches. This expansion of the public sphere undermines traditional notions of privacy, making it more difficult for individuals to protect their personal lives from external observation, thus represents both a new frontier and a battleground. Excessive data collection is a common problem, where apps gather more information than necessary, such as location, contacts, or browsing history, potentially violating user privacy. This can lead to unwanted profiling or the sale of data to advertisers without user consent. Additionally, insufficient consent mechanisms are prevalent; many applications software do not provide clear, explicit consent options for data collection and sharing, often hiding these details in lengthy privacy policies, leaving users unaware of how their data is being used. Inadequate data security is another critical issue, as some applications lack robust encryption and other security measures, making them vulnerable to data breaches that expose sensitive information like financial details or personal identifiers. Additionally, failure to delete user data is a concern, with some apps retaining personal data even after accounts are deleted or services are discontinued, which contravenes data retention and privacy laws.[7]

---

[7] Sowmiya B, Abhijith VS, Sudersan S, Sakthi Jaya Sundar R, Thangavel M, Varalakshmi P., *A Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19, National Center for Biotechnology Information,* March 11, 2021, *available at:* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7951128/ (last visited on Sep 13, 2024).

(a) Case Study on Recent Data Breach

When unauthorized parties gain access to sensitive or private information, such as social security numbers, bank details, medical records, or professional data like customer information, intellectual property, or financial records, termed as a data breach. While data breaches and cyberattacks often coincide, not every cyberattack results in a data breach. The term "data breach" specifically pointed out to instances where a security failure allows an unauthorized individual to access data.

(i) Boat Data Breach (April 2024)[8]

Details: A data leak affected 7.5 million boat customers of India. The information was available for sale on the dark web and could potentially be shared for free on Telegram in the future.

Impact: The breach heightened risks of financial fraud, identity theft, phone, and email scams.

Data Exposed: Customer names, addresses, email addresses, phone numbers, and customer IDs were exposed.

(ii) Covid-19 Data Breach (October 2023)[9]

Details: According to a News18 report, what could be the largest data leak in India has exposed the personal information of more than 81.5 crore citizens, allegedly obtained from the Indian Council of Medical Research (ICMR), and released online.

Impact: The data breach potentially exposes sensitive personal information, including Aadhaar and passport details, phone numbers, and addresses of millions, posing severe risks of identity theft and fraud.

---

[8] TOI Tech Desk, "*Name, address, contact number, email ID and other details of 7.5 million Boat customers leaked on Dark Web*", *The Times of India*, April 8, 2024, *available at* : https://timesofindia.indiatimes.com/technology/tech-news/name-address-contact-number-email-id-and-other-details-of-7-5-million-boat-customers-leaked-on-dark-web-claims-report/articleshow/109126826.cms (last visited on Sep 13, 2024).

[9] HT News Desk, *"Aadhaar details of 81.5 cr people leaked in India's 'biggest' data breach", Hindustan Times,* Oct. 30, 2023, *available at :* https://www.hindustantimes.com/technology/in-indias-biggest-data-breach-personal-information-of-81-5-crore-people-leaked-101698719306335.html (last visited on Sep 13, 2024).

Data Exposed: The exposed data includes Aadhaar and passport details, names, phone numbers, addresses, and Covid-19 test information of citizens registered with the ICMR.

(iii) Aadhar Card Data Leak (October 2018)[10]

Details: The Aadhaar system has faced multiple security lapses, with around 200 government websites accidentally exposing personal data in 2018, allowing unauthorized access to sensitive information. Fraudulent websites and phishing scams have also exploited these vulnerabilities. In one instance, Aadhaar details were sold for Rs 500 on WhatsApp, and a Jharkhand website leaked data of 1.6 million pension beneficiaries, highlighting ongoing systemic issues with data security.

Impact: The Aadhaar data breaches have undermined public trust in India's biometric ID system, exposing millions to identity theft, fraud, and unauthorized access to personal information. These incidents also highlight systemic flaws in government data management and security practices.

Data Exposed: The Aadhaar data breaches exposed sensitive information such as biometric data (fingerprints and iris scans), addresses, bank account details, and personal identification numbers.

(iv) Cambridge Analytica Scandal or Facebook Data Leak (2016)[11]

Details: Cambridge Analytica's contractors and employees gathered private Facebook data from 10 million users to sell psychological profiles to political campaigns. This was the largest known leak of Facebook data.

---

[10] Mardav Jain, *"The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment", the henry m. Jackson school of international studies, university of washington*, May 9, 2019, *available at :* https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/ (last visited on Sep 13, 2024).

[11] Nicholas Confessore, *"Cambridge Analytica and Facebook: The Scandal and the Fallout So Far", The New York Times,* April 4, 2018, *available at* : https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (last visited on Sep 13, 2024).

Impact: This scandal eroded public trust in Facebook and heightened concerns about data privacy. The fallout included a $5 billion fine and ongoing investigations into Facebook's data practices.

Data Exposed: Facebook users' names, locations, interests, friends list, and potentially even private messages. This data was used for voter profiling and political targeting without users' consent.

(v) LinkedIn Data Leak (2012)[12]

Details: In 2012, an enterprise divulged that invader had been filched 6.5 million passwords and advertised them on a Russian hacker forum. By 2016, it was discovered that the afore-mentioned intruder responsible for distributing My Space's data was also proposing the email addresses and passwords of approximately 165 million LinkedIn users for just 5 bitcoins, which was roughly equivalent to USD 2,000 at the time.

Impact: Many users were forced to change passwords across multiple services, causing significant inconvenience.

Data Exposed: With millions of email addresses and passwords exposed, users faced the risk of identity theft, unauthorized account access, and further exploitation across platforms where the same credentials were used.

7. Legal Framework Governing Right to Privacy in India

7.1 Observation of privacy as a fundamental right

(a) Kharak Singh vs. State of Uttar Pradesh[13]

This case is a crucial judgement in the evolution of the privilege to privacy in India. The apex court traced the first time the question of surveillance and its ramifications on an individual's fundamental rights. In this case, however, supreme court had not recognised right to privacy as a foundational privilege. The 6 judges' bench of Supreme

[12]Report of the Joint Committee on the Personal Data Protection Bill, 2019," 17th Lok Sabha Secretariat, Dec 16 2021, *available at:* https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf, (last visited on Sep 15, 2024).

[13] *Kharak Singh vs. State of Uttar Pradesh*, A.I.R. 1963 S.C. 1295 (India).

Court ruled that while the right to privacy is not explicitly mentioned in the Constitution, Article 21 could encompass the protection of personal liberty, which may include the privacy of an individual. The apex court further observed that home visitation by the police at night violated the personal liberty of the petitioner and was unconstitutional. The majority upheld the constitutionality of the other forms of surveillance.[14]

(b) People's Union of Civil Liberties v. Union of India (UOI)[15]

In 1991, PUCL, a civil rights organization, filed a public interest litigation in defiance of the central government since questioning the government's practice of intercepting telephone conversations. PUCL argued that unauthorized telephone tapping violates an individual's intrinsic to dignity and autonomy, as guaranteed under Article 21 of the Constitution of India. The Apex Court declared that the privacy is an integral aspect of the right to "life" and "personal liberty" organised under Article 21 of the Constitution, and the stated this claim cannot be abrogated "except according to procedure established by law". The Court upheld Section 5(2) of the Telegraph Act but imposed stringent conditions to ensure that telephone tapping is not misused. The judgment strengthened the legal framework for protecting individual privacy against unauthorized surveillance and established a benchmark for future cases concerning privacy in India.[16]

(c) Justice K.S. Puttaswamy (Retd.) v. Union of India[17]

The case was heard by a constitution bench of the Apex Court which delivered a unanimous judgment on August 24, 2017. The key points of the judgment are as follows:

(i) Right to Privacy as a Fundamental Right

The bench unequivocally determined that the entitlement to privacy is shielded as an inherent component of the life and personal liberty

---

[14] Supreme court of India, *available at:* https://main.sci.gov.in/judgment/judis/3641.pdf, (last visited on Sep 11, 2024).

[15] *People's Union for Civil liberties (Pucl) vs. The Union of India and Another*, (1997) 1 SCC 301.

[16] Supreme court of India, Dec 18, 1996, at 9-12, *available at:* https://main.sci.gov.in/judgment/judis/14584.pdf (last visited on Sep 13, 2024).

[17] *Justice K.S. Puttaswamy (Retd.) vs. Union of India*, (2017) 10 S.C.C 1 (India).

under Article 21 and as aspect of the liberties ensured by Part III of the Constitution. The judgment overruled previous decision of "*Kharak Singh case"* which had ruled that privacy was not a fundamental right.

(ii) Privacy as a Multifaceted Right:

The Court described confidentiality as a "multifaceted" right, encompassing various aspects such as bodily integrity, informational privacy, and the sanctity of private spaces and privacy includes the right to make personal decisions, the right to command one's personal information, also the privilege to be left alone.

(iii) Balancing Privacy with Other Rights:

While recognizing privacy as a basic right, the Court as well noted that it is not an unqualified right and may be subject to reasonable restrictions. Any law that infringes on the entitlement to privacy shall pass the test of proportionality, meaning that the law must pursue a legitimate aim, have a rational connection to the aim, and be the least restrictive means to achieve that aim.

7.2 Legislative Provisions

(a) The Information Technology Act (IT Act), 2000

The IT Act, 2000, is India's foremost legislation regulating electronic commerce and cybercrime. However, the Act itself does not explicitly address privacy as a comprehensive right, it contains several provisions related to information safety and privacy within the scope of electronic transactions and information handling. The key provisions of the IT Act, 2000, that relate to privacy are:

(i) Section 43A: Compensation for Failure to Protect Data

This section was inserted through the Information Technology (Amendment) Act, 2008, and holds entities accountable for handling sensitive personal data. Under Section 43A, if a body corporate (i.e., a company or organization) fails to effectuate appropriate compliant security protocols for the protection of sensitive personal data, and this results in wrongful loss or gain to any person, the affected person has the right to seek compensation.[18]

(ii) Section 66E: Punishment for Violation of Privacy

It criminalizes the act of intentionally recording, distributing, or sharing the visual depictions of a private area of any individual in the

[18] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

absence of their authorisation under conditions where the individual has a reasonable presumption of confidentiality. Punishment under this provision includes detention for up to 3 years or a monetary penalty of not exceeding Rs. 2 lakhs, or both.

(iii) Section 72: Breach of Confidentiality and Privacy

Section 72 of the Act prescribes unauthorized access to or disclosure of personal data. It penalizes government officers or service providers who, while executing their duties, have access to personal information and then disclose it non-consensual of the individual engaged. Sanction includes incarceration for not exceeding 2 years or a fine of up to Rs. 1 lakh, or both.[19]

(b) Intermediary Guidelines and Digital Media Ethics Code Rules, 2021[20]

These regulations, enacted pursuant to the IT Act, lay out guidelines for online platforms facilitators, web-based audio-visual platforms, and electronic news publishers, with a focus on ensuring data privacy and accountability. Facilitators are required to:

- Establish Complaint resolution mechanisms.
- Remove or disable content that violates secrecy.
- Deploy rigorous privacy controls to protect sensitive user information.

(c) Digital Personal Data Protection Act (DPDPA), 2023[21]

The Act of 2023 in India is an influential and major legislative Act designed to protect confidential information in the digital age. The key stipulations of the legislation are given below:

Definition of Personal Data (Sec 2 t): Any data that relates "to an identified or identifiable individual."

Personal Data Breach (Sec 2 u): It refers to any unapproved handling of sensitive records or unpremeditated events such as revelation, attainment, distribution, use, adaptation, obliteration, or access

---

[19] *Supra* note 17.

[20] *Available at* : https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf (last visited on Sep 14, 2024).

[21] *Available at* : https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf (last visited on Sep 14, 2024).

deprivation to non-public data that jeopardizes the confidentiality, integrity, or availability of that data.

Data Principal (Sec 2 j): It means the individual to whom the personal data relates.

Grounds for processing personal data (Sec 4): Personal data may be proceeded only when:

I. Data owner has granted his assent; or
II. for specific justifiable uses.

Consent (Sec 6): "Consent must be explicit, informed, and freely given. Individuals have the right to withdraw consent at any time."

Entitlement of Data Principal:

I. Entitlement to Data Access (Sec 11): Persons can request access to their personal records retained by organizations.
II. Entitlement to Correction (Sec 12): Persons can plea correction or updating of their data if it is false or insufficient.
III. Entitlement to Erasure (Sec 12): Individuals can plea to wipe out of their information when superfluous for its original intended use.
IV. Entitlement to nominate (Sec 14): A data owner has the right to appoint another person, as specified by regulations, who will, in the circumstances where data principal's death or inability, exercise their rights in accordance with the provisions of this Act and its associated rules.

Data Protection Officer (DPO): Organizations handling significant portions of sensitive data must designate a Data Protection Officer to administer abidance by the Act.

Data Protection Authority (DPA): The Act establishes a Data Protection Authority to oversee compliance, handle grievances, and enforce the provisions of the Act. The DPA has the power to investigate complaints, impose penalties, and issue directions to organizations.

Penalties and Enforcement: Penalties for non-compliance include fines and other sanctions. The Act outlines a framework for enforcement and legal recourse for individuals and organizations.

These provisions are designed to furnish a robust confidentiality protection model which balances the need to enhance for data integrity with the individual rights and liberties in the digital environment.

Critical Analysis of the DPDPA, 2023

While the DPDPA, 2023 is a major step forward, it has several limitations that raise constitutional and practical concerns. The most

debated issue is the 'legitimate uses' clause under Section 4, which allows the State to process personal data without consent for broad purposes such as national security, public order, and service delivery. Critics argue that these exceptions are not narrowly defined**,** and therefore risk creating an overbroad exemption that may dilute the fundamental right to privacy recognized in *Justice K.S. Puttaswamy case (2017)*.

The Supreme Court in *Puttaswamy* required that any restriction on privacy must follow the **proportionality test**—a legitimate aim, necessity, and least-restrictive method. However, the DPDPA does not expressly provide **independent oversight**, **prior judicial review**, or **proportionality safeguards** for State-based data processing. This creates a possibility that the law may be challenged on constitutional grounds.

Furthermore, the Act grants the Government wide powers to **exempt any State agency** from compliance. The absence of a strong, fully independent regulator (unlike the EU's Data Protection Authorities) also weakens enforcement.

(d) Digital Personal Data Protection Rules, 2025

The legal framework governing personal data protection in India has undergone significant advancement in recent months. In November 2025, the Government of India formally notified the **Digital Personal Data Protection Rules, 2025,** thereby giving practical effect to the Digital Personal Data Protection Act, 2023.[22] These Rules serve as the operational backbone of the statute and provide a comprehensive regulatory structure for both individuals and Data Fiduciaries.

The Rules strengthen the rights of data principals by outlining clear procedures related to **consent management, withdrawal of consent, correction and erasure of personal data,** and mechanisms for grievance redressal. They further mandate robust obligations on Data Fiduciaries, including **purpose limitation, strict data retention norms, encryption requirements, data minimisation**, and **mandatory breach-notification standards** to ensure accountability and transparency in the processing of personal data.

Importantly, the regulatory framework introduces an **18-month transition period** from the date of notification, allowing organizations

[22] Notification of the Digital Personal Data Protection Rules, 2025 by the Ministry of Electronics and Information Technology (MeitY).

adequate time to upgrade compliance systems and align their operational practices with statutory expectations. The Rules also formally establish the **Data Protection Board of India,** clarifying its powers, adjudicatory functions, and procedural guidelines for handling complaints and data-breach incidents. Special protections have also been incorporated for **processing children's data**, emphasising verifiable parental consent, restricted data profiling, and heightened security obligations.

Given these far-reaching developments, the article would greatly benefit from incorporating the **DPDP Rules, 2025**, as they represent the most recent and authoritative legal framework on digital privacy in India. Including these updates will ensure that the discussion reflects the current statutory position and aligns with contemporary regulatory expectations.

8. United States Governance Structure

The United States lacks comprehensive national data security laws, but there are some general federal regulations that offer data protection. Many states, due to the delegation of authority, have enacted their own data privacy laws. Following are the major secrecy and digital information security laws in the United States, outlining their scope, who they protect, and what they regulate.

(a) The Privacy Act of 1974[23]

Scope: National legislation that limits the disclosure of non-public data without the individual's written consent, except under specific exceptions, and establishes rights for persons to availability and rectify their files.

Who is Protected: U.S. inhabitants and legal permanent populace whose information is retained in federal agency data management systems

What is Regulated: It governs the assortment, utilise and dissemination of non-public information maintained by national entities in a system of records.

---

[23] U.S. Office of Special Counsel, The Privacy Act of 1974, *available at:* https://osc.gov/Pages/Privacy-Act.aspx#:~:text=The%20Privacy%20Act%20provides%20protections,relevant%2C%20timely%20or%20complete%3B%20and (last visited on Sep 14, 2024).

(b) Gramm-Leach-Bliley Act (GLBA) of 1999[24]

Scope: National law focused on how monetary organizations handle the gather, exert, and divulgence of consumers' restricted personal information.

Who is Protected: The GLBA protects consumers who engage with financial institutions.

What is Regulated: Financial institutions must provide annual privacy notices, offer opt-out options for sharing personal information, and implement security measures to safeguard it. They are prohibited from obtaining information through false pretences and face restrictions on sharing account details for marketing. Regulatory guidelines cover interagency coordination and FTC Act application.

(c) Children's Online Privacy Protection Act (COPRA) of 1998[25]

Scope: Federal law imposing requirements on websites and online services that collect data from children under 13, including obtaining guardian approval.

Who is Protected: Adolescents below the age of 13 using online services

What is Regulated: The Act necessitates websites and online services directed at children under age of 13 to obtain parental consent prior to accumulating, operating, or uncovering confidential content. Its directives explicit data handling policies, limits data collection, and enables parents to inspect or eliminate their children's information.

---

[24] Federal Trade Commission, Gramm-Leach-Bliley Act, *available at:* https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act (last visited on Sep 14, 2024).

[25] Federal Trade Commission, Children's Online Privacy Protection Rule ("COPPA"), *available at:* https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa (last visited on Sep 14, 2024).

(d) Electronic Communications Privacy Act of 1986 (ECPA)[26]

Scope: Federal law protecting virtual conversations during transmission and when filed electronically.

Who is Protected: Users of virtual communication systems (e.g., email, phone, internet)

What is Regulated: It protects wire, oral, and electronic communications from unauthorized interception, requires warrants for access to stored communications and subscriber data, and mandates court orders for pen registers which are tools designed to record or capture the dialled numbers and relevant associated information to which outgoing calls or communications are made by a specific individual, along with signal tracing tools used in investigations. It ensures privacy safeguards for data in transit, storage, and metadata.

(e) California Consumer Privacy Act of 2018 (CCPA)[27]

Scope: State law (California) that applies to businesses that collect personal information from California consumers.

Who is Protected: It protects California consumers, providing privacy rights to individuals residing in the state. Businesses subject to the CCPA must comply with these consumer protection laws.

What is Regulated: The law secures new privacy rights for California consumers, including:

Right to Know: Consumers may seek for report on what personal data is gathered, in what way it is utilised, and shared.

Right to Remove: Consumers may plea the removal of their individual data (with certain exemptions).

Right to Withdraw: Consumers may ask for to opt out of the sale or sharing of their non-public information.

---

[26] Department of Justice, United States Government, Electronic Communications Privacy Act of 1986 (ECPA), *available at:* https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#3-0 (last visited on Sep 14, 2024).

[27] State *of* California Department *of* Justice, California Consumer Privacy Act (CCPA), *March 13, 2024, available at:* https://oag.ca.gov/privacy/ccpa (last visited on Sep 14, 2024).

Right to Equal treatment: Businesses are prohibited from treating consumers unfairly or unfavourably for asserting their privacy rights.

9. United Kingdom Legal Framework

The UK's first privacy law, the "Data Protection Act 1984", was replaced by the 1998 Act, which implemented the EU Data Protection Directive. In 2018, the "Data Protection Act" was updated to align with the GDPR, enhancing individual rights and data protection standards. Following are the key UK legislation and guidelines applicable for the shielding of data and privacy:

(a) The Data Protection Act, 2018[28]

Description: It facilitates a wide-ranging structure for securing identifiable information in the UK. It incorporates GDPR provisions with additional UK-specific elements.

Key Provisions: Defines "personal data" and regulates its lawful processing. Companies operating in the UK must ensure data is collected, processed, and stored lawfully. They must obtain consent for data use intended to maintain sensitive details security, and provide mechanisms for data subject rights. Monetary penalty for non-adherence can extend up to £17,500,000 or 4% of undertaking's global turnover, whichever is higher.

(b) General Data Protection Regulation, 2016 (GDPR)[29]

Description: The GDPR is among the world's stringent privacy and cyber protection laws. It introduced by the European Union; its scope extends globally to all organizations that targets data from EU residents. Since its enforcement on May 25,

---

[28] *Available at:* https://www.legislation.gov.uk/ukpga/2018/12/contents (last visited on Sep 14, 2024).

[29] legislation.gov.uk, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation) (Text with EEA relevance), Done at Brussels, April 27, 2016 *available at*: https://www.legislation.gov.uk/eur/2016/679/contents?view=plain# (last visited on Sep 14, 2024).

2018, the GDPR has imposed tough repercussions for non-adherence, with fines to the extent of tens of millions of euros.

Key Provisions:

Data Protection Principles: Organizations must handle information legally, ethically, and clearly to specified objectives; restrict data intake; ensure data reliability; control data retention duration; and maintain details security and confidentiality. Data controllers are accountable for compliance.

Data Security: Suitable technical (such as, encryption, dual-factor confirmation) as well organizational (such as, staff mentorship, access limitation) actions must be in place. Data breaches must be reported within 72 hours unless data is encrypted.

(d) Privacy and Electronic Communications Regulations 2003 (PECR)[30]

Description: These Regulations are derived from European law, commonly termed as the 'e-privacy Directive.' PECR complements the GDPR by regulating electronic marketing communications and requiring organizations to gain consent for cookies and similar tracking technologies.

Key Provisions:

Marketing Communications: Businesses are required to secure approval in advance when delivering uninvited marketing emails, messages, or making marketing calls (unless the person is an existing customer).

Cookies: Consent is required before using cookies or other tracking technologies on websites.

Security Risks: If a significant security risk remains despite taking appropriate measures, entity must inform customers about the nature of the risk, steps they can take to protect themselves, and any potential costs involved in those protective measures.

---

[30] Information Commissioner's Office, What are PECR?, *available at:* https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/what-are-pecr/ (last visited on Sep 14, 2024).

(e) Network and Information Systems (NIS) Regulations 2018[31]

Description: These regulations, first introduced in 2018, to better protect essential services such as water, energy, and transport from cyber threats. These regulations, which mandate cybersecurity standards for companies providing critical services, will now be strengthened in response to increasingly sophisticated cyberattacks.

Key Provisions

- Recent proposals to update the NIS regulations (Dec 2022) aim to enhance the United Kingdom's cyber resilience by:
- Enlisting managed service providers to secure online supply networks.
- Enhancing cyber incident disclosure to regulatory authorities.
- Introducing a cost recovery model to uphold regulatory measures.
- Granting the government with the authority to amend regulations over time.
- Allowing the Information Commissioner to adopt a risk-focused strategy on risk assessment.

10. Comparative Weaknesses: DPDPA vs GDPR vs CCPA

Compared to the GDPR, India's DPDPA has **weaker protections** in three major areas:

(a) Enforcement Strength:

- GDPR has independent supervisory authorities with strong powers.

[31] Department for Digital, Culture, Media & Sport, The NIS Regulations 2018, April 20, 2018, *available at:* https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018#:~:text=The%20NIS%20Regulations%20provides%20legal,)%20and%20essential%20services%20(transport%2C (last visited on Sep 14, 2024).

- India's Data Protection Board is appointed by the Government, which raises concerns about independence in cases involving government data misuse.

(b) Data Subject Rights:

- GDPR grants broader rights such as the right to object, right to data portability, and right to restrict processing.
- DPDPA does not include these rights, limiting user control.

(c) Government Access to Data:

- Under the CCPA and GDPR, government access is subject to strict judicial oversight.
- DPDPA exemptions allow broad State access without similar safeguards.
- Thus, while India's framework is inspired by global models, its enforcement and safeguards are comparatively limited.

11. Should India Adopt Measures as in Developed Countries?

India, as a rapidly digitizing economy, is grappling with its own data privacy challenges. However, India should consider adopting measures from developed countries like the USA and UK, but with careful adaptation to its unique socio-economic and legal context. Developed nations have implemented advanced privacy compliance standards namely "the General Data Protection Regulations (GDPR)" in Europe and the "California Consumer Privacy Act (CCPA)" in the USA, which provide robust protections for personal data, including users' written consent, data minimization, and the right to be forgotten. These frameworks have set a high standard for data privacy laws globally, and India could benefit from incorporating similar principles to address its growing digital economy.

12. Recommendations and Suggestions

12.1 Integrating Nissenbaum's Contextual Integrity into Privacy Protection

Digital platforms create hybrid spaces where the boundary between public and private is blurred. Therefore, privacy cannot be protected through generic or one-size-fits-all solutions. Drawing upon Helen Nissenbaum's principle of *contextual integrity*, privacy protections must align with the norms of the specific environment in which information is shared. Data shared in one context (e.g., for medical treatment, employment verification, banking, or social networking)

should not be repurposed or transferred to another context without explicit justification and safeguards. This approach allows India's privacy framework to respond to the complex reality of Big Data, targeted advertising, algorithmic decision-making, and state surveillance.[32]

Based on this theoretical lens, the following recommendations are proposed:

12.2 Recommendations for Users (Context-Specific Guidance)

Instead of generic behavioural advice, users need **context-aware strategies** that match the specific platform or activity in which data is being shared.

(a) Social Media Context

Users should adjust privacy settings to control the audience of their posts and ensure that information intended for a private circle is not unintentionally exposed to wider networks. Oversharing is often a result of platform design, which encourages disclosure; therefore, users must evaluate whether the platform's context aligns with how they expect their data to be used.

(b) E-Commerce and Online Services

Platforms often collect data for service improvement but reuse it for targeted marketing or profiling. Users should review permissions carefully and restrict data-sharing to purposes consistent with the service they are using. Where possible, they should opt out of cross-platform tracking.

(c) Workplace and Educational Platforms

In professional or institutional settings, surveillance tools (attendance apps, CCTV, keystroke monitoring, biometric attendance) must be evaluated against the legitimate expectations of the workplace context. Users should be informed about data-retention policies and raise objections when monitoring exceeds what is necessary for job performance or safety.

(d) Health and FinTech Applications

Highly sensitive data such as health records, biometrics, and financial activity should only be shared with platforms that follow strong

---

[32] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford Univ. Press 2010); Helen Nissenbaum, Privacy as Contextual Integrity, 79 *Wash. L. Rev.* 119 (2004).

encryption and transparent data-use policies. The expectation of confidentiality in these contexts is stronger than in social media or e-commerce, and users should demand proportional safeguards.

12.3 Recommendations for Organisations/Government (Context-Aware Policymaking)

(a) Contextual Integrity as a Legal Standard

Indian regulators should incorporate contextual integrity into the interpretation of "legitimate uses" under Section 4 of the DPDPA. Any data processing beyond consent should be valid only when it respects the original context in which the information was provided. This will prevent wide and vague exemptions that could undermine the *Puttaswamy* judgement standard of proportionality.

(b) Sector-Specific Privacy Rules

Instead of broad, uniform rules, India should adopt sector-based privacy norms similar to the GDPR's specialised frameworks (such as for health data, children's data, and biometric data).

- Health data should have strict confidentiality norms.
- Workplace data should require transparency and proportionality.
- Social media companies must follow clear limits on behavioural advertising.

This reduces the risk of over-broad "legitimate use" exceptions.

(c) Privacy by Design and Data Minimisation

Organisations should embed privacy into system architecture—collect only the minimum data necessary, segregate data by purpose, and prevent "function creep," where information gathered in one context (e.g., KYC) is reused in unrelated contexts (e.g., targeted advertising).

(d) Algorithmic Accountability

AI-driven profiling and automated decision-making should be regulated, requiring companies to explain:

- what data is used,
- for what purpose,
- how user rights will be protected.

This is crucial in financial lending, insurance pricing, and recruitment platforms where opaque algorithms can create unfair outcomes.

(e) Public Awareness Based on Context, Not Generic Tips

Digital literacy campaigns must shift from giving simplistic advice (e.g., "do not post online") to explaining how different platforms use

data, how cookies track cross-platform behaviour, and how "consent" can be manipulated through dark patterns.

13. Conclusion

In an era where personal data is treated as a commodity, it is imperative to reassess privacy rights to ensure the protection of individual dignity and autonomy. As digital platforms and surveillance technologies become increasingly powerful, privacy laws must adapt to meet new challenges. Privacy protection in the digital era cannot rely on outdated notions of secrecy or the idea of being "left alone." As Nissenbaum's contextual integrity highlights, privacy is preserved only when information flows follow the norms of the specific context in which they were shared. The dual aim of data privacy and protection is not only to defend the rights of individuals but also to hold organizations accountable for safeguarding the personal information entrusted to them. Ensuring robust data privacy practices fosters a more secure digital environment, where users can engage with digital services confidently, knowing their information is protected and their privacy respected. The balance between innovation and privacy can be achieved, but only if policymakers, corporations, and individuals work together to establish a system that prioritizes human dignity over profit.