YourLawArticle

Open Access Law Journal, ISSN (O): 3049-0057

Editor-in-Chief – Prof. (Dr.) Amit Kashyap; Publisher – Reet Parihar

Digital Privacy In The Age Of Surveillance:- " India's It Rules Vis-à-Vis U.S. Data Protection Regime

Amanpreet Kaur, LL.M., School of Law, Lovely Professional University

Published on: 19th September 2025

Abstract

In the present scenario, as human interaction is increasing online, privacy protection is becoming a primary concern. The struggle to control personal information is becoming a challenging task for the legal framework. The government and companies collect and share the data of an individual without explicit consent. The kind of surveillance done by technologies like AI threatens individual rights, but for the protection of the data protection laws taking place. By the way, the law information of an individual available online is protected.

There are tools like virtual private networks (VPNs) which can help individual to protect their own data. Personal information in the business sector plays a vital role as it helps business units to know their customers effectively. No doubt, the government have a valid reason to collect data, that is, the reason for crime prevention. Digital privacy aids in the prevention of cybercrime, such as identity theft. In other countries like the U.S.A., there is a California Consumer Privacy Act (CCPA), which aims to protect the data of individuals. Data privacy is the safety and truthful utilisation and handling of personal information. Ensuring proper statistical safety reduces breaches of sensitive information, identity theft, and cybercrimes.

KEYWORDS: *- Virtual Private Network (VPNs), data privacy, cyber crimes*

INTRODUCTION

The concept of privacy has existed since ancient civilizations, where individuals sought to protect personal belongings, identity, and dignity. In early societies, privacy often revolved around familial and domestic spheres, with the household serving as a private domain distinct from the public realm. For instance, in ancient Rome, privacy was linked to notions of personal identity and social status, with the Latin term privatus denoting what was withdrawn from the community and reserved for individual use. Roman citizens expressed concerns about intrusion into private life, not only by fellow citizens but also by the state. Similarly, in ancient Greece, the distinction between the oikos (private household) and the polis (public life) underscored the importance of separating the individual's intimate space from collective obligations.[1]

Philosophers also articulated the value of personal space and autonomy. Aristotle's writings reflected an awareness of the tension between public life and private existence, while later Enlightenment thinkers like John Locke and John Stuart Mill emphasized individual liberty, laying intellectual foundations for modern privacy discourse. Locke's theory of natural rights and Mill's advocacy of personal freedom both influenced legal traditions that would later recognize privacy as an aspect of human dignity and autonomy. [2]

In the modern era, the discourse on privacy intensified with technological advances, particularly from the mid-20th century. The emergence of mass communication technologies, such as radio, photography, and later television, challenged traditional notions of what could be considered "private." In 1890, Samuel Warren and Louis Brandeis, in their seminal Harvard Law Review article "The Right to Privacy," described privacy as the "right to be let alone," signaling the first major attempt to articulate privacy as a legal right in response to invasive technologies like instant photography and mass media.

By the mid-20th century, the expansion of bureaucratic systems, government record-keeping, and corporate data collection gave rise to new anxieties about personal information being stored, categorized, and used without consent. Alan Westin, in his influential work Privacy and Freedom (1967), [3]defined privacy as the "claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others." His formulation became a cornerstone in privacy scholarship, as it linked privacy directly to individual autonomy and control over personal data, while also recognising the growing threat posed by information-processing technologies.[4]

With the rise of computers and databases in the 1940s–1960s, privacy concerns deepened. Information

[1] Jill Lepore, *The Secret History of Wonder Woman* (Knopf 2014) 33.
[2] Hannah Arendt, *The Human Condition* (University of Chicago Press 1958) 28–31.
[3] Alan F Westin, *Privacy and Freedom* (Atheneum 1967).
[4] John Locke, *Two Treatises of Government* (Cambridge University Press 1988 [1689]); John Stuart Mill, *On Liberty* (Penguin Classics 1985 [1859]).

once fragmented across paper records could now be centralized, analyzed, and cross-referenced with unprecedented ease. This raised the possibility of misuse, surveillance, and loss of individual control over personal identity. For example, government census records and credit histories were increasingly digitised, fueling debates about "dataveillance", a term later popularised by Roger Clarke to describe systematic monitoring through data collection. [5]

By the 1990s, the emergence of the internet and e-commerce further amplified these risks. The shift from analogue to digital interactions meant that nearly every online activity like emails, purchases, social connections created data trails. Corporations began monetizing personal information through targeted advertising, while governments expanded surveillance capacities in the name of security. The shaping of platforms such as Facebook in the early 2000s exemplified this transformation, where personal information became not only a matter of private autonomy but also a valuable commodity in the global digital economy. These developments laid the foundation for today's debates around data protection, surveillance, and privacy in the digital age.[6]

HISTORICAL ASPECT

EARLY CONCEPT OF (PRE-1990S): -

The concept of privacy, particularly the protection of personal information and individual autonomy, has roots in ancient civilisations. Even the Romans expressed concerns about identity and the intrusion of others into private life. In the modern era, Alan Westin's influential work Privacy and Freedom (1967) defined privacy as the right of individuals to control their personal information, a definition that shaped much of the discourse on privacy and technology during the 1940s to 1960s.

With the advent of computers and databases, new challenges emerged. The centralisation and storage of data increased the risk of misuse, as personal information could be collected, processed, and shared on a scale never seen before.

The Beginning of the Internet Age (1990s)

The widespread adoption of the internet and the rise of e-commerce in the 1990s revolutionized data collection and sharing practices. Platforms such as Facebook marked a turning point, transforming how personal information was exchanged and commodified in the digital sphere. In the present stage of technological advancement, developments such as artificial intelligence, big data analytics, and machine learning continue to reshape the landscape of privacy, creating both opportunities and risks for individuals and societies alike.

[5] Roger Clarke, 'Information Technology and Dataveillance' (1988) 31 *Communications of the ACM* 498.
[6] Alan F Westin, *Privacy and Freedom* (Atheneum 1967).

PRIVACY

Privacy refers to an individual's right to control access to their personal space, information, and communications. It includes freedom from intrusion and the ability to decide what to share. Roger Clarke (2005) identified four dimensions of privacy: [7]

1. Privacy of Personal Communications – also called "interception privacy," concerning the confidentiality of conversations.
2. Privacy of Personal Data – referred to as "data privacy" or "information privacy."
3. Privacy of Personal Behaviour – relating to habits, political beliefs, and religious practices, often described as "media privacy."

SURVEILLANCE

Surveillance refers to the systematic observation of individuals, groups, or environments, often involving the close monitoring of personal details, behaviours, communications, and social interactions. It is primarily employed to manage, influence, or control the subjects under observation, with the intention of ensuring compliance, maintaining security, or gathering intelligence. The concept of surveillance is broad and encompasses a range of methodologies, from simple observation to the use of advanced technological tools such as CCTV cameras, biometric tracking, online data monitoring, and artificial intelligence-powered systems.

Surveillance can be classified into two main types:

1. Mass Surveillance: Mass surveillance refers to the systematic and comprehensive monitoring of large populations without necessarily targeting specific individuals. This form of surveillance collects and analyses data from a broad group of people, often through digital platforms, telecommunications, public space monitoring, or data aggregation systems. Mass surveillance is typically justified by states on grounds of national security, crime prevention, or public health, but it raises significant concerns regarding privacy, civil liberties, and the potential for abuse.[8]

2. Targeted Surveillance: Targeted surveillance focuses on monitoring particular individuals, locations, or activities. This type of surveillance is more selective and usually applied when there is a specific suspicion or reason to investigate a person or entity. Law enforcement agencies often employ targeted surveillance to track criminal activity, prevent terrorism, or collect evidence in ongoing investigations. While it is generally more precise than mass surveillance, it still requires careful legal oversight to prevent violations of privacy rights and ensure proportionality. [9]

---

[7] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.
[8] David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001) 5.

[9] Kirstie Ball and Frank Webster (eds), *The Intensification of Surveillance: Crime, Terrorism and Warfare in the 21st Century* (Routledge 2003) 23.

Both forms of surveillance have expanded dramatically with the advent of digital technologies, raising important ethical, legal, and social questions. For instance, while surveillance can enhance security and enable effective law enforcement, excessive monitoring may lead to the erosion of personal freedoms, the creation of a "chilling effect" on free expression, and the misuse of sensitive personal data. [10]

INDIAN CONSTITUTIONAL APPROACH

Under the Indian constitutional framework, the protection of data and privacy has evolved significantly through judicial pronouncements and legislative developments. While the Constitution of India does not explicitly mention the term "privacy," Indian courts have interpreted existing fundamental rights to encompass privacy, especially under the ambit of Article 21, which guarantees the right to life and personal liberty.[11]

Case Study: Justice K.S. Puttaswamy vs Union of India (2017)

In this landmark judgment, the Supreme Court of India unequivocally recognized privacy as a fundamental right intrinsic to Article 21. The Court emphasized that privacy encompasses multiple dimensions, including informational privacy, bodily integrity, and decisional autonomy, and serves as a cornerstone for the exercise of other fundamental rights, such as freedom of speech and expression and freedom of association. This judgment has become the foundational authority for subsequent data protection and privacy laws in India.[12]

AMERICAN CONSTITUTIONAL APPROACH

The United States of America lacks an explicit constitutional provision for privacy. Instead, privacy protections have emerged through judicial interpretations, statutory enactments, and sector-specific regulations. The U.S. approach is characterized by a sectoral and fragmented regime, with distinct laws addressing specific areas of data protection rather than a unified framework.[13]

(A) Sectoral Nature of U.S. Privacy Laws

The U.S. federal system enacts privacy protections for particular sectors or categories of information:

1. Health Insurance Portability and Accountability Act (HIPAA) – Governs the protection of health data for covered entities, including healthcare providers and health plans.
2. Gramm-Leach-Bliley Act (GLBA) – Focuses on safeguarding sensitive financial information held by financial institutions.[14]
3. Children's Online Privacy Protection Act (COPPA) – Protects the personal data of children under

[10] Clive Norris and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV* (Berg 1999) 47–48.
[11] Constitution of India 1950, art 21.
[12] *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.
[13] Daniel J. Solove and Paul M. Schwartz, Information Privacy Law (6th edn, Wolters Kluwer 2021) 15–20.
[14] Gramm-Leach-Bliley Act, Pub L No 106–102, 113 Stat 1338 (1999).

13 collected online. [15]

(B) Fragmented System

The American privacy landscape is further complicated by a fragmented approach, with federal, state, and even local regulations creating a patchwork of rules:

1. **State-Level Laws –** For instance, California's Consumer Privacy Act (CCPA) provides comprehensive privacy rights for consumers within the state.
2. **Patchwork of Regulations –** This fragmented system results in overlapping and sometimes inconsistent rules across different sectors and jurisdictions.

Case Studies

1. **Griswold vs Connecticut (1965) –** The U.S. Supreme Court recognized a constitutional right to privacy, specifically marital privacy, drawing this right implicitly from the "penumbras" of various amendments, including the First, Third, Fourth, Fifth, and Ninth Amendments. [16]
2. **Carpenter vs United States (2018) –** The Court held that the government's collection of historical cell phone records, which can track a person's movements, constitutes a search under the Fourth Amendment, thereby requiring judicial oversight.[17]

These cases illustrate how U.S. privacy rights, although not explicitly codified in the Constitution, have been judicially developed to respond to evolving technological challenges and societal expectations

COMPARATIVE ANALYSIS BETWEEN INDIA AND THE UNITED STATES OF AMERICA:-

The Digital Era, driven by surveillance and technological innovation, has created legal frameworks that protect individual privacy. The three approaches shaped by the unique constitutional traditions and socio-political priorities are being revealed by three distinct approaches.

In the United States, privacy rights have largely evolved through judicial interpretations of the Fourth Amendment and the due process clause. Landmark judgments held in warren vs Brandeis and Katz vs United States have historically the need to safeguard individuals from intrusive state action.

In India, the stage present a hybrid model that has increasingly evolved over recent years. In the landmark judgement of Puttaswamy vs Union of India created a privacy as a fundamental right under Article 21, making it important for the protection from both governmental and corporate intrusions. India is making a legislative framework, given by the Digital Personal Data Protection Act, that creates a bridge with the state's economic and security concerns.

SUGGESTIONS: -

[15] Children's Online Privacy Protection Act, 15 USC §§ 6501–6506 (1998).
[16] *Griswold v Connecticut* 381 US 479 (1965).
[17] *Carpenter v United States* 585 US ___ (2018).

Data privacy is important for protecting sensitive information,such as personal identification of data, financial details, health records, etc from misuse.

The steps that can help to protect the personal information online:-

1. Limited data Exposure:- Beaware about sharing personal information on social media and other online portals. The websites has to be checked before providing any data.

Review privacy setting and consider the potential risks before posting.

2. Practice good cyber hygiene :- This include effective and unique passwords for every accounts to reduce the risk of personal information to be leaked out.

3. software updates :- It is necessary to keep a check on all the applications and antivirus software programs that they are updated which will help in providing protection of data online.

4. Support privacy enhancing technologies:- Utilize tools such as virtual provate network (VPN's) and privacy focused web browsers to minimize tracking and data collection.

5. Privacy measures:- By using privacy measures can make technology more effective. Strong privacy measures protect against data breaches that can lead to significant financial losses for Individual as well as for organizations.

CONCLUSION

Surveillance has brought different challenges with varied responses to collect and manage its impact from different regions. The various approaches are rooted in their constitutional, historical and cultural priorities. United State depends upon a patchwork of sector-specific regulations and Fourth Amendment protections, result in a fragmented privacy framework. India, influenced by the landmark Puttaswamy judgment, is shaping its approach with the DPDP Act, 2023 which seeks to balance individual privacy with state and corporate interests.