© JULY 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1719397

Right To Privacy: Tracing the Evolution of Privacy in the Digital Age

ANKUSH SINGLA
Bhartiya Vidyapeeth Deemed University

Abstract- ***Privacy, considered by many as a basic right, has always been evolving and changing in the digital world and will keep changing at an even faster pace. Over the years the concept of the right to privacy has been tested, stretched and reimagined in the context of technology changes in America's case law. This paper examines the right to privacy in four general periods: common law era, constitutional era, first digital disruption era, and the era of ubiquitous surveillance, algorithmic profiling and artificial intelligence. The paper discusses critically some of the important cases of the United States Supreme Court, the European Court of Human Rights and the Supreme Court of India that have affected the privacy jurisprudence in the respective jurisdictions. It examines data protection laws in the EU (e.g., the General Data Protection Regulation (GDPR)), India (e.g., the Digital Personal Data Protection Act, 2023) and some of the major challenges and issues for privacy in the platform economy, biometric surveillance and AI, and assesses their relevance and effectiveness. The paper highlights three tensions that are present in modern privacy law, namely privacy vs security in a mass surveillance world, privacy vs innovation in a data economy and privacy vs enforcing privacy rights in a broader power dynamic, such as a technology platform. It adopts comparative constitutional law to craft a reconceptualised notion of privacy in the current digital world as shaped by the principle of dignitary autonomy, a risk-based notion of the proportionality of data-processing, and structural duties of non-state and state actors.***

Keywords: Right to Privacy, Digital Age, Surveillance, Data Protection, Fundamental Rights, GDPR, Digital Personal Data Protection Act 2023, Informational Self-Determination, Bodily Autonomy, Cyber Law, Artificial Intelligence, Constitutional Morality.

I. INTRODUCTION

1.1 The Paradox of Privacy in the Digital Age

This is a definition of privacy: Privacy is "the most comprehensive of rights, and the right most valued by civilised men. But in the 21st century the most precious of the rights is in its worst danger for its existence. Personal data is being produced, captured, manipulated and monetised at an unprecedented pace and scale due to the exponential growth of digital technologies including social media, smartphones, cloud computing, the Internet of Things, biometric technologies and artificial intelligence, which has caused a change in the nature of the flow of personal data and fundamentally shifted the assumptions that underpinned privacy law.

The paradox of privacy in the digital age is manifest in the following reality of today: people willingly give up huge amounts of private information to commercial platforms for free services and then are subjected to massive and sophisticated state surveillance apparatuses. It is a state that has been described by scholars as the ‘surveillance society,' the ‘transparent society,' and the ‘data panopticon . The exposed person is seen by the corporate platforms, State agencies and algorithmic systems and has less actual ability to determine the conditions of exposure in each of the formulations.

1.2 Research Problem and Significance

This paper has taken up as its main research problem the fundamental failure of current privacy law regime to adequately meet the qualitative shift in the character of privacy risks in the digital era. Current law, built around the "reasonable expectation of privacy" doctrine outlined in Katz v. United States and the three-part test developed in later decisions, was developed for a time when access to information was more limited and discrete. This research is important because it adds to the burgeoning scholarly literature on the need for a reconceptualised privacy framework adequate to the demands of the digital age – one that is based not merely in procedural consent mechanisms, but in substantive dignitary protection,

structural power accountability and genuine informational self-determination

1.3 Research Questions

The central research questions that guide this paper are the following:

i How has the conceptual and legal content of the right to privacy evolved from its common law roots to its reconceptualisation in the digital age?
ii What are the main structural threats to privacy in the digital age and what has been the response of legal systems?
iii Are the existing data protection frameworks including GDPR and the DPDPA 2023 adequate enough to address the contemporary privacy challenges?
iv What normative reforms are needed to improve privacy protection in the age of artificial intelligence and mass surveillance?

1.4 Research Methodology and Structure

This paper is based on the doctrinal method of legal research, in which comparative constitution analysis and technological assessment along with normative legal theory are used. The research relies on primary sources such as constitutional provisions, legislation, judicial rulings of various jurisdictions, and official reports, and secondary literature from the top law reviews, human rights journals, and interdisciplinary technology law scholarship. This paper is divided into eight substantive parts, which follow this introduction.

II. HISTORICAL FOUNDATIONS OF THE RIGHT TO PRIVACY

2.1 The Common Law Genesis: Warren and Brandeis

The modern idea of privacy has been traced to the 1890 Harvard Law Review article “The Right to Privacy” authored by Samuel D. Warren and Louis D. Brandeis,' which was prompted by the rise of the instantaneous photograph and the sensationalist press. Warren and Brandeis contended that the doctrine of the common law already acknowledged a general right ‘to be let alone' through the doctrines of property, contract and breach of confidence, and that those courts should explicitly state this as a doctrinal principle.

Spacial and reputational privacy were the focus of the Warren-Brandeis conception of privacy, which primarily concerned the protection of privacy in the domestic sphere and the unauthorised publication of private facts. Though of historical significance, this formulation was inevitably constrained. It saw privacy as a negative right ("freedom from") rather than a positive right of informational self-determination. It didn't deal with the systemic nature of privacy violation in an institutionalized era of data processing.

2.2 Early Judicial Recognition: The American Experience

The landmark case of Griswold v. Connecticut (1965), which, in total, involved the First Amendment, Third Amendment, Fourth Amendment, Fifth Amendment and Ninth Amendment rights, has been decided by the United States Supreme Court that there is a “zone of privacy” protected by these combined amendments that the State could not have a lawful right to intrude into. In Katz v. United States (1967), Justice Harlan's concurring opinion further developed the constitutional aspects of privacy by formulating the 'reasonable expectation of privacy' test that has been the predominant standard for Fourth Amendment jurisprudence for more than five decades. The reproductive side of constitutional privacy was expanded in Roe v. Wade (1973); the side of decisional privacy was expanded in Lawrence v. Texas (2003); which established a comprehensive constitutional right to individual autonomy in intimate personal decisions.

2.3 The European Tradition: Privacy as a Fundamental Human Right

Privacy in the European tradition is predominantly regarded as one of the basic rights of the individual, based on human dignity. Article 8 of the European Convention on Human Rights (ECHR) which guarantees the right to respect for private and family life, home and correspondence , has produced a large body of jurisprudence from the European Court of Human Rights (ECtHR). The subsequent cases of Landmark v United Kingdom (1976), Malone v

United Kingdom (1984), Halford v United Kingdom (1997) and S and Marper v United Kingdom (2008) brought to a head the large number of issues surrounding the expanding protection of Article 8 in relation to telephone tapping, workplace monitoring, DNA databases and the retention of personal data by the police.

2.4 The Indian Constitutional Framework: Privacy as a Fundamental Right

India's constitutional path of evolving the right to privacy from a "penumbral" to an "explicit" right took six decades beginning from the epochal 1963 case of Golak Nath v. State of Punjab, and culminating in the nine-judge Constitution Bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The previous cases were doctrinally inconsistent: a few of them found the right to privacy to be a part of personal liberty guaranteed by Article 21 of the Constitution, while others had held that there was no constitutional right to privacy, such as M.P. Sharma v. Satish Chandra (1954).

The Constitution Bench in Puttaswamy unanimously ruled that the right to privacy in Article 19, 14 and 21 of the Constitution of India is a Fundamental Right. Justice D.Y. Chandrachud's opinion captured that ‘heterogeneity' is 'an intrinsic recognition' which is fundamental to the realization of individual personality and dignity, highlighting the importance of privacy. The Court recognized three types of constitutional privacy – privacy of the person (bodily integrity), privacy of information (informational self-determination) and privacy of choice (decisional autonomy).

III. PRIVACY IN THE DIGITAL TRANSITION ERA (1990s-2010s)

3.1 The Internet and the Emergence of Digital Privacy Threats

With the commercialization of the internet in the 1990s, the era of threats to privacy entered a new stage; the unprecedented ability to collect, aggregate and cross-reference personal data at a low cost. The first internet privacy controversy was about cookies, commercial e-mail (spam) and the unauthorized release of personal data in online transactions. The United States Congress responded with a series of sectoral statutes: the Electronic Communications Privacy Act, 1986, the Video Privacy Protection Act, 1988; the Children’s Online Privacy Protection Act, 1998, and the Health Insurance Portability and Accountability Act, 1996. One critique of this approach on a sectoral basis has been that one can find large gaps and inconsistencies in the regulations.

3.2 The European Data Protection Framework: From 1995 Directive to GDPR

Europe has been responding to the threat of digital privacy with guarantees of full, rights-based data protection regulations. The EU Data Protection Directive of 1995 laid the foundation for personal data protection in the EU. The GDPR – the General Data Protection Regulation – was a complete overhaul of the European data protection system and took effect on 25th May 2018. The GDPR introduced significant innovations, such as the need to obtain explicit consent for data processing, the ‘right to be forgotten', the ‘right to data portability', the duty to conduct data protection impact assessments, the ‘data protection by design and by default' and tougher enforcement mechanisms, such as fines of up to 20 million euros or 4% of global annual turnover.

In the digital world the ‘right to be forgotten' was enshrined in law in 2014, when the Court of Justice of the European Union (CJEU) ruled in Google Spain SL v. Agencia Espanola de Proteccion de Datos, requiring search engine operators to remove search results that link to personal data that is outdated, irrelevant or excessive.

3.3 Mass Surveillance and the Post-Snowden Legal Landscape

In 2013, Edward Snowden's revelations about the National Security Agency's mass surveillance programs (PRISM, XKeyscore, Tempora, and more) marked a turning point in the ongoing privacy debate.Edward Snowden's revelations about the National Security Agency's mass surveillance programs (PRISM, XKeyscore, Tempora, and others) were a watershed moment in the global privacy debate in 2013. Legal reactions were sizeable in several regions. The USA FREEDOM Act, 2015

limited the bulk telephone metadata collection programme of the NSA in the United States. In Big Brother Watch v. United Kingdom (2021), the ECtHR found that the UK's bulk interception of communications was in violation of Article 8 of the ECHR in several respects. The UN Human Rights Council passed Resolution 28/16, which states that "the same rights that people have offline must also be protected online.

The Puttaswamy case in India was a case where the Court was specifically dealing with the restrictions on the State's surveillance, and it ruled that the State's action in restricting the right to privacy must be in line with the requirements of legality, legitimate aim, and proportionality.

IV. CONTEMPORARY PRIVACY THREATS IN THE DIGITAL AGE

4.1 The Data Economy and the Commodification of Personal Information

The "business model" of the modern "Internet economy" is the extraction and exploitation of personal data. Platforms such as Google, Facebook (Meta), Amazon and Twitter (X) provide ‘free' services in exchange for access to their users' personal data that is processed, analysed and sold to advertisers, political campaigns and other commercial entities. The model of 'surveillance, capitalism' is an approach that views human experience as the fuel used to extract behavioural information – and crunch it into 'prediction products' that foresee and shape human behaviour. The consent-based approach of data protection law is inherently inadequate for the opacity of algorithmic data processing, and for the complexity of platform terms of service.

4.2 Artificial Intelligence, Machine Learning, and Algorithmic Privacy

Existing law is not robust enough to protect privacy in a qualitatively new way presented by the technologies of artificial intelligence and machine learning. Machine learning algorithms can make highly sensitive personal inferences, such as health conditions, sexual orientation, political beliefs, financial vulnerability, psychological characteristics etc., from seemingly non-sensitive behavioural data, creating an 'inferential privacy violation' that is not captured by the existing data protection frameworks.

Facial recognition technology is a particularly acute challenge to privacy. In public areas, facial recognition technology can be used to identify and track individuals without their awareness or consent. Facial recognition systems incorrectly identify people, especially women and people of colour, exacerbating concerns of discriminatory impacts. The EU Artificial Intelligence Act, 2024 prohibits the use of real-time, remote biometric identification by law enforcement in public places, except in limited cases.

4.3 Biometric Data and the Unique Dignity Interests at Stake

The importance of biometric data in privacy law lies in its profound linkage to the individual and the fact that it is immutable and permanent. In the Aadhaar Case (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2018), the Supreme Court of India struck down the Aadhaar biometric identification system, which is the world's largest biometric database. The Court has confirmed the constitutional validity of the Aadhaar scheme in its main applications and invalidated some provisions that allowed for use of Aadhaar for authentication by private parties.

4.4 Social Media, Self-Disclosure, and the Privacy Paradox

The spatial and contextual principles that underlie privacy law have been severely challenged by the use of social media. Helen Nissenbaum, calls this concept ‘contextual integrity’ and defines it as ‘Privacy norms are context dependent.’ That is to say, when information is flowing it is "appropriate" if it is in accordance with the norm of the place from which the information was originally published. Users who talk about privacy concerns but then spew personal information on social media websites is not a sign of consent – it's a structural result of the power dynamic between platform p roviders and social media users.

V. THE RIGHT TO PRIVACY: JUDICIAL MILESTONES ACROSS JURISDICTIONS

5.1 United States Supreme Court: From Katz to Carpenter

The 'third-party doctrine' developed in Smith v. Maryland (1979) — has been particularly damaging in the digital context, which held that people do not have a reasonable expectation of privacy in information voluntarily disclosed to third parties. In United States v. Jones (2012), Justice Sotomayor's concurring opinion cast doubt on the continued relevance of the third-party doctrine in the digital age, as the Supreme Court slowly began to turn its back on the doctrine.

The historic Carpenter v. United States (2018) marked the biggest shift in digital privacy doctrine in Fourth Amendment history. In his majority opinion, Chief Justice Roberts explained why the third-party doctrine was not applicable to the digital world anymore, finding that the "information collected by cell-site location devices can be used to achieve near perfect surveillance" and that it therefore f alls under the Fourth Amendment.

5.2 The Right to Be Forgotten: Google Spain and Its Legacy

One of the more contentious and far-reaching changes in digital age privacy law is the 'right to be forgotten' (now the 'right to erasure' under GDPR Article 17). The internet's permanence and ability to be indexed, searched and accessed at any time means that people are allowed to forget less now than in the pre-digital world – and that forgets can be created and perpetuated indefinitely if the internet does not destroy a person's reputation. The CJEU's Google Spain ruling has set out the guidelines for the right to delist links from search engines to information that is outdated, irrelevant or disproportionate to the dignity and reputation of the data subject.

5.3 India: Puttaswamy and the Post-2017 Privacy Jurisprudence

Justice K.S. Puttaswamy (Retd) v Union of India is India's most extensive judicial interpretation of the right to privacy. The six concurrences of the nine Justices present differing, but similar, conceptions of constitutional privacy. According to Justice D.Y. Chandrachud, ‘preservation of personal intimacies, sanctity of family life, marriage, procreation, the home and sexual orientation are at the core of privacy.

Since the Puttaswamy decision, the constitutional contours of digital privacy have been further elaborated. In Anuradha Bhasin v. Union of India (2020), the Supreme Court noted that the right to access the internet is an integral part of the right to privacy, which is enshrined in Articles 19(1)(a) and 21 of the Constitution. The Court's comments on targeted surveillance with spyware in Re: Pegasus Project further elaborated on the constitutional framework for assessing surveillance by the State in the digital era.

VI. COMPARATIVE DATA PROTECTION FRAMEWORKS

6.1 The General Data Protection Regulation (GDPR): Architecture and Assessment

The GDPR is the world's most comprehensive and influential data protection legislation. It extends beyond its borders and has been the de facto worldwide guide for data protection, leading to the 'Brussels Effect' of EU data protection on global data protection. Article 5 of the GDPR outlines the principles of the GDPR, including lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. The regulation also provides a detailed list of data subject rights.

The five-year implementation of GDPR has brought a lot of success stories and challenges. The regulation has shown its deterrent potential, through enforcement actions against major technology firms such as the 1.2 billion euro fine against Meta by the Irish Data Protection Commission in 2023. Yet, this has been criticized for being inconsistently applied across different member states and for the lack of consent to be the main legal grounds for pro cessing in the platform economy.

© JULY 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1719397

6.2 India's Digital Personal Data Protection Act, 2023

The path of the country towards a unified personal data protection legislation has been a long and rocky one. In 2018, the Justice B.N. Srikrishna Committee submitted its report and a draft Personal Data Protection Bill, which was reviewed by a Joint Parliamentary Committee. Finally, the Digital Personal Data Protection Act (DPDPA), 2023 was passed by Parliament, which is a significantly less rights-centric and Government-friendly framework, as compared to that recommended by the Srikrishna Committee. The DPDPA 2023 provides a framework of consent and sets up the Data Protection Board of India as the adjudicatory and enforcement body. There are a number of major drawbacks, which critics have pointed out: Firstly, broad State exemptions mean that data principals are not subject to any meaningful control over government data processing. Secondly, the rights a data principal can assert under GDPR are much stronger than those under the DP Act.

6.3 The California Consumer Privacy Act and the United States Landscape

California, without having a comprehensive federal data protection law, has become the regulatory leader within the United States. The California Consumer Privacy Act (CCPA) of 2018, combined with the California Privacy Rights Act (CPRA) of 2020, ensures California residents have the rights to know, opt out of data sale, delete and correct personal information. The fragmented character of the US data protection law, which consists of sectoral federal laws and a comprehensive state-level law has been strongly criticized as causing regulatory complexity and substantial gaps in protection coverage. To date, there has been no legislative consensus on a comprehensive federal privacy law, such as the American Data Privacy and Protection Ac t, which was introduced in 2022.

6.4 Comparative Overview of Data Protection Frameworks

Feature	GDPR (EU)	DPDPA 2023 (India)	CCPA/CPRA (California)
Scope	All personal data of EU residents; extraterritorial reach	Digital personal data; limited territorial scope	Consumers in California; revenue/data volume threshold
Lawful Bases	Six bases incl. consent, legitimate interest, contract	Consent + deemed consent for legitimate uses	Opt-out model; no prior consent required for collection
Individual Rights	Access, rectification, erasure, portability, objection, no-profiling	Access, correction, erasure, grievance redressal	Know, delete, correct, opt-out of sale, portability
State Exemptions	Narrow exemptions; State bound by most provisions	Broad; Government exempt for 'public interest'	Government entities broadly exempt
Max Penalty	EUR 20M or 4% global turnover	INR 250 crore per instance	USD 7,500 per intentional violation
Enforcement Body	National DPAs; EDPB at EU level	Data Protection Board of India	California Privacy Protection Agency

VII. STRUCTURAL TENSIONS IN CONTEMPORARY PRIVACY LAW

7.1 Privacy versus Security: The Surveillance State Dilemma

The divide between privacy and national security is the most politicized aspect of current privacy law. States claim that mass surveillance is essential to protect against terrorism, serious crime and threats to national security. Critics of mass surveillance, including privacy experts, argue that mass surveillance is a disproportionate abridgement of the fundamental rights, and that it has been proven by practical experience to be an ineffective counterterrorism tool. The tension must be resolved in law in a strict application of the proportionality

principle: which is that any interference with the right to privacy must be prescribed by law, serve a legitimate aim, be necessary in a democratic society, and be subject to effective oversight and redress mechanisms.

In Centrum for Rattvisa v. Sweden (2021), the ECtHR reaffirmed that mass interception of communications is not in principle incompatible with Article 8 of the ECHR, provided it is subject to an adequate legal framework, is subject to independent monitoring, and mechanisms for redress are in place.

7.2 Privacy versus Innovation: The Data Economy Dilemma

The other structural tension in digital age privacy law is between privacy protection and technological innovation. The use of large-scale analyses of personal and behavioural data is on the basis of some of the most significant applications of the data economy, such as medical AI, personalised education, climate modelling, and optimising urban mobility. Differential privacy, federated learning, homomorphic encryption, and synthetic data generation are among the many examples of privacy-preserving technologies that show that many valuable analytical applications of personal data can be achieved without compromising individual privacy. But what is the question here? Is it possible to innovate with privacy protection, or is it possible for the bottom lines of dominant technology platforms to align with actual privacy protection?

7.3 Privacy and Equality: The Discriminatory Dimensions of Data Processing

No society is equally affected by privacy breaches in the digital world. Marginalised communities and vulnerable groups are at greater risk of privacy breaches by both the State and commercial data processing. Personal data has been shown to be used in algorithmic decision-making systems that have discriminatory effects on already disadvantaged populations in areas such as employment, credit, housing, healthcare and criminal justice. The new research area of 'discriminatory data practices' has been created in order to better conceptualize privacy law to account for both the individual's right to control his or her own personal data and the systemic and collective nature of instances o f algorithmic privacy violation.

VIII. TOWARDS A RECONCEPTUALISED PRIVACY FRAMEWORK FOR THE DIGITAL AGE

8.1 Beyond Consent: Towards Dignitary Privacy Protection

The limits of consent as the basis of digital privacy protection are now widely acknowledged in the legal literature and in policy. An alternative foundation is provided by the dignitary theory of privacy, that has been developed by Jeffrey Rosen, Daniel Solove, and others. The dignitary view of privacy has a strong basis in the view that privacy is a requirement of human dignity and personhood that must be respected as a public law obligation, whether or not the individual has given his consent to its violation.

8.2 A Risk-Based and Proportionality-Centred Regulatory Approach

A privacy framework for the digital age needs to be based on the risks in the context of the nature of data processing, and should apply appropriate levels of regulatory scrutiny to different types of data processing activities to reflect the different levels of privacy risks. The proportionality principle, which was also imported from European constitutionalism, provides a normatively-justified test for assessing the legitimacy of interference with privacy – the interference has to serve a legitimate purpose; the interference has to be necessary to achieve the legitimate purpose; the legitimate purpose has to be proportionate to the cost of privacy; and there has to be effective protection and remedies. The framework outlined in the Supreme Court of India's recent Puttaswamy decision – which it had established as the prism for analyzing constitutional privacy in the case – offers a principled basis to resolve the tensions between privacy and security, privacy and innovation, and privacy and equality which typify modern privacy law.

8.3 Structural Obligations and Platform Accountability

Solutions to the privacy problems in the digital age must be structural, imposing obligations on dominant

technology platforms, rather than rights and remedies. These individual consent-based and post-hoc regulatory approaches do not sufficiently account for the ability of incumbents to exercise monopolistic market power and impose conditions on how the data is shared. The new paradigm of 'privacy as infrastructure' (PPI) provides a strong theoretical base for this structural approach to the regulation of privacy. Environmental law has obligations that are placed on polluters whether or not there is formal consent, and privacy law should have obligations placed on data processors, where the processing poses unacceptable risks to individual dignity and societal welfare.

IX. CONCLUSION

The right to privacy has come a long way from being a simple remedy in private law for unwanted attention from the media in 1890 to being a multi-faceted fundamental right which is an essential part of human dignity, autonomy and democratic self-governance in the 21st century. This development has been fuelled by a dialectical process between the emergence of new and more serious privacy threats, on the one hand, and legal innovation, on the other, which has been mandated to rethink privacy in the light of emerging threats repeatedly.

There are four key findings that result from the analysis in this paper. First, the right to privacy in the digital age is a multidimensional right – spatial privacy, informational privacy, decisional privacy and dignitary privacy – and policies that only tackle one or two of these dimensions will systematically fail to cover individuals in the digital age. Second, the consent lawful basis of data protection law is structurally not adequate for the platform economy and needs to be complemented — if not replaced — by substantive obligations of data processors who dominate the market. Thirdly, the privacy/security dichotomy is not the best one to reconcile these values with privacy but the one to develop policies and regulations that are security oriented, innovative and equality-enhancing, and pro-privacy at the same time. Fourth, there is a need for more coordination and convergence between global privacy governance, particularly with regard to extraterritorial privacy effects of the data economy in all countries.

Data protection legislation must be comprehensive and rights-based to address all elements of digital privacy threats, meaningful structural obligations on dominant technology platforms must be put in place, enhanced protection for biometric and sensitive data is needed and truly independent enforcement bodies must be created. Judicial decision making should be dynamic and attentive to context, grounded in theories and understandings from contextual integrity, dignitary privacy, and comparative constitutionalism, and constantly evolving over time to maximise constitutional privacy norms as technology advances. There is a need for regulatory authorities to become aware of the potential for substantive privacy harm of the platform economy and AI and to develop more sophisticated, technically savvy and enforcement-oriented solutions to data protection than is currently the case, one based on mere procedural compliance.

Here privacy is not a regulatory technical matter. It is an underlying condition of democratic society, one condition which must be fulfilled prior to the fulfillment of all the others and it is a precondition in an age where the power of information is supreme. Thus, the right to privacy in the digital world is the right of individual and foremost the right of the collective democratic people. The Supreme Court of India in Puttaswamy said privacy is a 'right to be different' of an individual, a right to stand against the tide of conformity. The right needs to be constitutionally protected in the digital world!

REFERENCES

[1] Olmstead v. United States, 277 U.S. 438 (1928) (Brandeis J., dissenting).

[2] David Brin, The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom? (Perseus Books, 1998).

[3] David Lyon, Surveillance Society: Monitoring Everyday Life (Open University Press, 2001).

[4] Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs, 2019) ch. 1.

[5] Ibid., 361 (Harlan J., concurring).

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

[7] Terry Hutchinson & Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17 Deakin Law Review 83.

[8] Neil M. Richards & Daniel J. Solove, 'Privacy's Other Path: Recovering the Law of Confidentiality' (2007) 96 Georgetown Law Journal 123.

[9] Samuel D. Warren & Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

[10] Julie E. Cohen, 'What Privacy is For' (2013) 126 Harvard Law Review 1904, 1906.

[11] Daniel J. Solove, 'A Taxonomy of Privacy' (2006) 154 University of Pennsylvania Law Review 477.

[12] Ibid., per Douglas J.

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

[14] Roe v. Wade, 410 U.S. 113 (1973), subsequently overruled by Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022).

[15] Lawrence v. Texas, 539 U.S. 558 (2003).

[16] European Convention on Human Rights (1950), Article 8.

[17] Malone v. United Kingdom (1984) 7 EHRR 14.

[18] Handyside v. United Kingdom (1976) 1 EHRR 737.

[19] Halford v. United Kingdom (1997) 24 EHRR 523.

[20] S and Marper v. United Kingdom (2009) 48 EHRR 50.

[21] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

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

[23] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.

[24] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, para 323 (Chandrachud J.).

[25] Ibid., para 295.

[26] Paul Schwartz, 'Privacy and Democracy in Cyberspace' (1999) 52 Vanderbilt Law Review 1607.

[27] Viktor Mayer-Schonberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think (John Murray, 2013) 14.

[28] Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848 (1986).

[29] Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936 (1996).

[30] Children's Online Privacy Protection Act, 15 U.S.C. Section 6501 et seq. (1998).

[31] Video Privacy Protection Act, Pub. L. 100-618, 102 Stat. 3195 (1988).

[32] Peter P. Swire & Lauren Faith Rein, 'US Protection of Personal Information: Current Approaches and the Long-Term Challenge' in Graham Greenleaf (ed.), Asian Data Privacy Laws (OUP, 2014).

[33] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (wp243rev.01, 2017).

[34] GDPR, Articles 6, 7, 17, 20, 25, 35 and 83.

[35] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data.

[36] Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos [2014] ECR I-317 (CJEU).

[37] Orla Lynskey, 'Deconstructing Data Protection: The Content and Function of the Right to Data Protection in Light of the CJEU's Case Law' (2014) 63 ICLQ 569.

[38] Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA and the Surveillance State (Metropolitan Books, 2014).

[39] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act (USA FREEDOM Act), Pub. L. 114-23 (2015).

[40] Big Brother Watch v. United Kingdom (2021) 74 EHRR 20.

[41] UN Human Rights Council, Resolution 28/16, 'The Right to Privacy in the Digital Age' (26 March 2015).

[42] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, para 180 (Chandrachud J.).

[43] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75.

[44] Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press, 2015).

[45] Lorrie Faith Cranor, 'Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice' (2012) 10 Journal on Telecommunications and High Technology Law 273.

[46] Alessandro Acquisti, Curtis Taylor & Liad Wagman, 'The Economics of Privacy' (2016) 54 Journal of Economic Literature 442.

[47] Sandra Wachter & Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2019 Columbia Business Law Review 494.

[48] Sandra Wachter & Brent Mittelstadt, 'A Right to Reasonable Inferences' (2019) 2019 Columbia Business Law Review 494.

[49] Clare Garvie, Alvaro Bedoya & Jonathan Frankle, 'The Perpetual Line-Up: Unregulated Police Face Recognition in America' (Georgetown Law Center on Privacy & Technology, 2016).

[50] Regulation (EU) 2024/1689 (Artificial Intelligence Act), OJ L, 12.7.2024.

[51] Joy Buolamwini & Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) Proceedings of Machine Learning Research 81.

[52] EU AI Act, Articles 5, 10, 26.

[53] Paul Schwartz & Daniel Solove, 'Reconciling Personal Information in the United States and European Union' (2014) 102 California Law Review 877.

[54] Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar Case), (2019) 1 SCC 1.

[55] Ibid., para 389 (Sikri J.).

[56] Ibid., para 389 (Sikri J., majority opinion).

[57] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press, 2010).

[58] Alessandro Acquisti & Jens Grossklags, 'Privacy and Rationality in Individual Decision-Making' (2005) 3(1) IEEE Security & Privacy 26.

[59] danah boyd, It's Complicated: The Social Lives of Networked Teens (Yale University Press, 2014) 57.

[60] Ibid., 418 (Sotomayor J., concurring).

[61] United States v. Jones, 565 U.S. 400 (2012).

[62] Smith v. Maryland, 442 U.S. 735 (1979).

[63] Carpenter v. United States, 585 U.S. 296 (2018).

[64] Ibid., 320 (Roberts CJ.).

[65] Ibid., 320 (Roberts CJ., majority opinion).

[66] GDPR, Article 17 (Right to Erasure / Right to be Forgotten).

[67] Jonathan Zittrain, 'Don't Force Google to Forget' The New York Times, 14 May 2014.

[68] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

[69] Re: Pegasus Project, Writ Petition (Civil) No. 314 of 2021 (Supreme Court of India, 27 October 2023).

[70] GDPR, Article 5 (Principles Relating to Processing of Personal Data).

[71] Anu Bradford, The Brussels Effect: How the European Union Rules the World (Oxford University Press, 2020) 149.

[72] GDPR, Articles 15-22.

[73] Data Protection Commission (Ireland), Decision re Meta Platforms Ireland Limited, DPC-E-2-2022 (22 May 2023).

[74] Lilian Edwards, 'The EU Data Act: A Solution in Search of a Problem?' (2022) 22 Computer Law Review International 133.

[75] Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy,

Empowering Indians (Ministry of Electronics and Information Technology, Government of India, 2018).

[76] Digital Personal Data Protection Act, 2023 (No. 22 of 2023).

[77] Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, Report (Lok Sabha Secretariat, December 2021).

[78] Vrinda Bhandari & Rishika Sahgal, 'An Analysis of the Digital Personal Data Protection Act, 2023' (2023) 58(42) Economic and Political Weekly 17.

[79] Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Information & Communications Technology Law 65.

[80] California Privacy Rights Act (Proposition 24), Cal. Civ. Code Section 1798.99.10 et seq. (2020).

[81] California Consumer Privacy Act, Cal. Civ. Code Section 1798.100 et seq. (2018).

[82] American Data Privacy and Protection Act, H.R. 8152, 117th Congress (2022).

[83] Aharon Barak, Proportionality: Constitutional Rights and their Limitations (Cambridge University Press, 2012) ch. 4.

[84] European Union Agency for Fundamental Rights, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU (FRA, 2017) 45.

[85] Centrum for Rattvisa v. Sweden (2021) 74 EHRR 38.

[86] Marietje Schaake, The Tech Coup: How to Save Democracy from Silicon Valley (Princeton University Press, 2024) ch. 5.

[87] Cynthia Dwork, 'Differential Privacy: A Survey of Results' (2008) Lecture Notes in Computer Science 4978.

[88] Ruha Benjamin, Race After Technology: Abolitionist Tools for the New Jim Code (Polity, 2019) ch. 1.

[89] Dorothy E. Roberts, 'Digitizing the Carceral State' (2019) 132 Harvard Law Review 1695.

[90] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (St Martin's Press, 2018) ch. 2.

[91] Khiara Bridges, 'Privacy Rights and Public Families' (2011) 34 Harvard Journal of Law & Gender 113.

[92] Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (Harvard University Press, 2018) 23.

[93] Jeffrey Rosen, The Unwanted Gaze: The Destruction of Privacy in America (Random House, 2000); Daniel J. Solove, Understanding Privacy (Harvard University Press, 2008).

[94] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, para 310 (Chandrachud J.).

[95] Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (Oxford University Press, 2019) 212.

[96] Lina M. Khan, 'Amazon's Antitrust Paradox' (2017) 126 Yale Law Journal 710.