INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

RIGHT TO PRIVACY: AN ANALYSIS OF THE LEGAL FRAMEWORKS IN THE USA, UK, AND INDIA

AUTHOR - ASHMITA GUPTA*, ANKIT RAJ** & UJJWAL PRAKASH**

* ASSISTANT PROFESSOR AT LAW STUDENT, LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY, DEHRADUN

** STUDENTS AT LAW STUDENT, LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY, DEHRADUN

BEST CITATION - ASHMITA GUPTA, ANKIT RAJ & UJJWAL PRAKASH, RIGHT TO PRIVACY: AN ANALYSIS OF THE LEGAL FRAMEWORKS IN THE USA, UK, AND INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (2) OF 2026, PG. 184-191, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/VPOB1226

Abstract

The history of humankind is as old as the right to privacy. It is one of the most important issues of the day and is changing along with the dynamics of human society. Unquestionably, social media represents a significant danger to the right to privacy and is the new vitality of this generation. This right encompasses a broad scope, which causes it to become intertwined with other rights like the freedom to information. The two are not balanced, which creates privacy issues that require adjustments. This essay aims to provide an overview of the legal problems and the methods that different countries have chosen to address them. The rights to privacy are fraught with such complexity. delicately woven, thus care must be taken to maintain its integrity and safeguard the core of our fundamental human right the right to privacy.

Introduction:

The notion of privacy, if it has any meaning at all, is a person's right, married or single, to be free from unjustified government interference. In the modern world, the conversation about privacy has become more and more prevalent, and the landscape is rapidly changing. There is a push to protect people's privacy from invasion, especially in the era of information technology, where the threat of violation is ubiquitous. This paper provides a comparative examination of the Right to Privacy in India, the United States, and the United Kingdom. It also explores recent court rulings and the development of privacy rights in these countries. The recognition of the right to privacy as an international standard is an intriguing feature to think about. The scope of privacy includes the right to data protection, the integrity of one's home, marriage, family life, sexual orientation, and all aspects of one's existence that are subject to unauthorized interference by public or private entities. International movements and protests have generated a wave of recognition for the necessity of establishing a "Right to Privacy." An attempt is being made to compare laws between countries, examining their approaches to providing their citizens with privacy rights.

Right to Privacy: A Comprehensive Study

Although not explicitly stated in many national constitutions, courts around the world have recognized the right to privacy by interpreting other constitutional clauses. Some dimensions of privacy include informational privacy, physical privacy, spatial privacy, and decisional privacy. Informational privacy concerns people's power over their personal information and their ability to restrict its gathering, use, and sharing. Individuals are entitled to privacy under

several international agreements and declarations, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[415]

Privacy rights are seriously threatened by technologies such as online tracking, biometric data gathering, facial recognition, surveillance cameras, and facial recognition. Additionally, the lines separating the public and private domains have become increasingly hazy due to the widespread use of social media and the internet, raising concerns about data ownership, permission, and digital privacy. The right to privacy in one's physical environment, such as one's house, includes the ability to be alone and exercise control over it. This right of people to freely choose their lifestyle, religion, and mode of expression is known as decisional privacy.

Global legal frameworks attempt to achieve a balance between the right to privacy and competing interests such as public health, law enforcement, and national security. A number of jurisdictions have enacted data protection laws and regulations to regulate the collection, use, and sharing of personal information, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) of the European Union. Courts frequently apply the proportionality test, which weighs the importance of the government's objective against the invasion of an individual's rights, to decide whether privacy violations are justified.

Government monitoring and business data activities are not the only threats to privacy rights. Individuals' ability to enjoy privacy can also be influenced by cultural norms, economic disparities, and social customs. Marginalized groups such as minorities, immigrants, and the economically disadvantaged may suffer from disproportionate privacy intrusions for which there is little or no legal recourse due to systemic imbalances.

In addition to legal protections, technological improvements bring both opportunities and challenges for privacy. Users can protect their information and preserve their anonymity online with the use of anonymization techniques, encryption, and privacy-enhancing technologies (PETs). However, concerns about ubiquitous surveillance, algorithmic discrimination, and the degradation of privacy in public spaces are brought about by new technologies such as big data analytics, artificial intelligence (AI), and the Internet of Things (IoT).

Encouraging digital literacy and enlightening individuals about their privacy rights are essential steps in guaranteeing privacy protection in the digital age. Encouraging people to make informed judgments about their data sharing habits and advocating for open data regulations are two ways to mitigate privacy risks.

In an increasingly interconnected world, the right to privacy is a complex and dynamic concept that is essential for maintaining individual freedom, autonomy, and dignity. Academic institutions, civil society organizations, and privacy advocates play a significant role in shaping public opinion, influencing the creation of public policy, and holding businesses and governments accountable for invasions of privacy. In order to guarantee individuals' private rights and the confidentiality of their personal data and autonomy in the physical and digital domains, a combination of regulatory safeguards, technological measures, and public education is required.

Right to Privacy in India

In our nation, as far back as 1954, the Supreme Court, in the cases of M. P. Sharma & others vs. Satish Chandra, District Magistrate, Delhi & others (1954 AIR 300, 1954 SCR 1077), and later in 1964 in Kharak Singh vs. State of Uttar Pradesh (1964) 1 SCR 332, rejected the assertion of a fundamental right to privacy, stating it wasn't guaranteed under the Indian Constitution.

[415] Universal Declaration of Human Rights art. 12, Dec. 10, 1948; International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

However, in 2017, a unanimous decision by a nine-member Constitution Bench in Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, (2017) 10 SCC 1, recognized the Right to Privacy as inherent in fundamental rights under Articles 19 and 21, overturning previous judgments.[416] Consequently, it's now firmly established that Right to Privacy is a fundamental right in our legal framework.

In the case of R. Rajagopal v. State of T.N. 1994 SCC (6) 632, the Supreme Court clarified this idea further and affirmed the right to privacy's implicit status as a component of the life and liberty protected by Article 21. It asserted that individuals have the right to protect their privacy concerning personal matters, and any unauthorized publication about such matters without consent, except when based on public records, would be a violation of privacy and subject to legal action.[417] This norm has exceptions, such as when someone willingly participates in public conversation or when there are public records at issue. In addition, it is essential to protect the victim's privacy in cases of sexual assault or other comparable violations.

The law of torts in India is not codified; instead, it is founded on common law ideas that were mostly taken from English tort law. Judicial precedent and statutes pertaining to damages and civil procedure which have been modified to fit the Indian context determine its applicability.

Indian courts have dealt with a range of situations when the Right to Privacy under Article 21 has been violated. For example, the Andhra High Court held in Rayala M. Bhuvaneswari vs Nagaphanender Rayala AIR 2008 AP 98 that recording a wife's conversations without her consent violates her fundamental right to privacy under Article 21 and makes the evidence inadmissible in court.

The Supreme Court's decision in People's Union of Civil Liberties (PUCL) v. Union of India 1971 (1) SCC 301, a case in which a Public Interest Litigation attempted to prevent indiscriminate telephone tapping, should be mentioned. The court affirmed that the right to privacy includes phone calls, whether they are held at home or at work, acknowledging that they are an essential part of private life. The judge declared: "Telephone conversations often carry intimate and confidential content, integral to modern life and increasingly facilitated by mobile devices. As such, they form a crucial component of an individual's private sphere. Consequently, the right to privacy extends to telephone conversations in both personal and professional settings. Unauthorized telephone tapping would thus violate Article 21 of the Indian Constitution, unless conducted under legally established procedures."[418]

In Mr. X v. Hospital Z (1998) AIR 1999 SC 495, (1998) 8 SCC 296, the court addressed a conflict between fundamental rights, including the right to privacy, ruling that the right promoting public morality or interest should prevail. In this case, the court deliberated whether the hospital violated the appellant's privacy by disclosing their HIV-positive status. The court opined:

"Beyond the Fundamental Rights guaranteed under Article 21, including the Right to Life, individuals have the right to pertinent information affecting their health and well-being. Thus, the disclosure of a life-threatening illness, like HIV/AIDS, to a potential partner is necessary for safeguarding their right to lead a healthy life. In cases of conflicting Fundamental Rights, such as privacy versus public health, the court will enforce the right that advances public interest, as moral considerations cannot be disregarded."

Furthermore, the Madras High Court case of R. Sridhar vs R. Sukanya And Ors. (2005) 1 MLJ 214, drawing from the apex court's ruling in Gobind v. State of Madhya Pradesh and Anr., (1975) 2 SCC

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

[417] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632 (India).

[418] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301 (India).

148, highlighted the right to privacy in marital disputes under the Hindu Marriage Act 1955. The court emphasized the need for in-camera proceedings to preserve privacy and barred media coverage.

The right to privacy in India encompasses various aspects, including reproductive autonomy, as seen in State of Maharashtra v. Madhukar Narayan Mardikar AIR 1991 SC 207, where the court protected the privacy of a prostitute. Legislation such as the Right to Information Act, 2005, upholds privacy rights, as evident in Section 8(1)(j), which safeguards personal information from unwarranted disclosure.

However, challenges persist, notably in the digital realm, with concerns over Aadhaar's potential privacy breaches and the absence of comprehensive data protection laws. The Information Technology Act 2000 addresses some privacy concerns, penalizing unauthorized data disclosure under Sections 43A and 72A. Despite attempts to enact a Data Privacy and Protection Act in 2017, legislative efforts have faltered, leaving citizens vulnerable to privacy infringements.

Unsolicited telephone calls present a prevalent violation of privacy, necessitating regulations to safeguard against such intrusions. Judicial intervention is imperative to establish robust privacy protections, particularly in light of evolving privacy dimensions like data privacy, medical confidentiality, and digital surveillance. Balancing privacy rights with national interests and holding both state and private entities accountable for data protection is crucial in our increasingly digitized society.

Right to Privacy in USA

As previously mentioned, Louis Brandeis and Samuel Warren first articulated the concept of the right to privacy under the United States Constitution in their renowned essay published in the Harvard Law Review in 1890. While the term "privacy" is not explicitly stated in the Constitution, various fundamental safeguards are enshrined in the Bill of Rights.

Since 1965, the United States Supreme Court has acknowledged the right to personal privacy and certain other forms of privacy under the Constitution, including protections found in the First, Fourth, and Fifth Amendments, as well as within the Bill of Rights Penumbras, the Ninth Amendment, and the concept of liberty outlined in the first section of the Fourteenth Amendment. Additionally, the Children's Online Privacy Protection Act of 2000 safeguards children's privacy rights in the United States.

The case of Boyd v. United States marked the first instance where privacy concerns were brought to the forefront. In Katz v United States, the Supreme Court introduced the "reasonable expectation of privacy test," which asserts that the Fourth Amendment ensures the right to privacy if an individual anticipates privacy (subjective) and if society deems such expectation as reasonable (objective).[419]

Moreover, in Smith v. Maryland, the US Court acknowledged the limitations of the Katz principles, particularly in scenarios that cannot be accommodated within the framework of the Fourth Amendment.

The right to privacy attained "fundamental" status according to the US Supreme Court's ruling in Roe v. Wade, wherein any infringement by the state must be justified by compelling public interest. Lawrence v. Texas, a 2003 case, upheld the privacy rights of two homosexual individuals and invalidated Texas' sodomy ban, exemplifying this principle.

Presently, Ron Wyden, Rand Paul, and eleven other Senators have introduced the USA Rights Bill aimed at reforming the National Security Agency (NSA) surveillance program, one of the most potent forms of government surveillance. This initiative seeks to enhance the civil liberties protected by the US Constitution.

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

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Right to Privacy in UK

The concept of Right to Privacy as it pertains to the United Kingdom. Article 8 of the Human Rights Act of 1998, which deals with the respect for private and family life, is relevant to bring up.[420] This clause clearly protects a person's right to privacy with regard to their private life, relationships with family members, place of residence, and correspondence (including emails, letters, and phone conversations). Article 8 grants people the freedom to live their lives in private, unhindered by the government. The concept of 'private life' has been interpreted broadly by UK courts, covering characteristics like sexual orientation, lifestyle choices, physical appearance, and bodily autonomy. It also includes the right to manage who has access to one's body, therefore situations like being exposed in public or having medical treatments done against one's will are prohibited. Furthermore, the right to create a personal identity and build connections is included in private lifeThis right protects people against unjustified meddling by the media and by the government, protecting private information such as medical records, diaries, and official documents, which must be handled securely and shared only with permission unless there are special circumstances.

Every person of the United Kingdom is entitled to the autonomy to foster family connections free from state interference. Interestingly, "family life" in the UK includes relationships such as those between foster families, unmarried partners, and adopted children and parents. Nonetheless, there are limitations to the right to privacy in the UK. There are times when the right to one's own house, correspondence, and private and family life may be violated by the government or public authority.

Only when it can be proven to be legitimate and necessary for purposes like maintaining public safety, national security, preventing crime, or defending the rights and liberties of others is such intervention acceptable. Goodwin & I v. United Kingdom [2002], a seminal decision relevant to this setting, saw the European Court of Human Rights consider problems transgender people faced with regard to their rights to marriage and a private life. The ruling was a major step in recognising the rights of transgender people, who were not previously recognized in the context of marriage under UK law.

The Court ruled that such treatment violated both the right to private life and the right to marry. Consequently, the UK Government later enacted the Gender Recognition Act 2004, establishing measures to address discrimination against transsexual individuals.

The Right to Privacy: An Expansive Perspective

Embedded within the right to privacy lies the concept of the 'Right to be Forgotten', a notion that entails the removal of publicly available personal information from internet platforms, search engines, databases, and other public forums, provided such information is no longer relevant or applicable. This idea was first brought to light in the case of Google Spain vs. Maria Costa Gonzalez, where Maria Costa contended that the exposure of an auction notice for his foreclosed property from 1998 in a Google search constituted a violation of his privacy rights. He argued that both the newspaper and Google had mishandled his personal data. Upon review by the Spanish Data Protection Authority, it was determined that while the newspaper routinely updates its news content and is not obligated to retract past publications, Google, as a processor of user data, was instructed to remove Maria Costa's private information.[421] Subsequently, this concept found resonance in various Indian cases as well. In Jorwar Singh Mundy vs. Union of India, an American citizen, Jorwar Singh Mundy, sought to overturn the Delhi High Court's judgment in an NDPS Act case, where he had been acquitted of all charges. He claimed that his reputation was damaged by the judgment's

[420] Human Rights Act 1998, c. 42, art. 8 (UK).

[421] Google Spain SL v. Agencia Española de Protección de Datos, Case C-131/12, 2014 E.C.R. I-0000 (Court of Justice of the European Union).

public accessibility. According to the Delhi High Court, the Right to be Forgotten gives people the ability to have documents, videos, or photos of themselves removed from certain online records. This protects them from being found by search engines. It emphasizes the ability of the person to repress irrelevant prior experiences from their life.
But the idea presents a problem because it conflicts with the right to information. Therefore, it is necessary to create a careful balance between these rights by limiting both the public's access to sensitive personal data and the right to information. In the age of technology and the internet, where information can be shared with just a click, this issue takes on a fundamental importance. False accusation incidents can be extremely damaging to a person's reputation, especially if the material is still available to the public. The Right to be Forgotten is an expansion of the right to privacy and should be carefully considered because it may have implications for many aspects of a person's life.

Current Privacy-Related Events

Examples of privacy-related incidents happen all the time. The WhatsApp privacy policy, for instance, has caused anxiety among data regulators and privacy specialists. Users were required to approve this revised policy, which described WhatsApp's intention to collect a variety of data, including IP addresses, usage patterns, device specifications, contact details, and profile details. Notably, the policy made clear WhatsApp's aim to allow third parties including Facebook corporations to read communications that users and businesses trade on the network. This development's extended data collection and sharing practices aroused the attention of regulatory organizations and privacy experts. Even while users of digital platforms sometimes accept privacy terms without giving them careful thought, the revised WhatsApp policy resulted in a sizable customer exodus, motivated by worries that Facebook would be able to view private messages. The urgency of enacting data privacy laws in India was highlighted by this circumstance, especially in light of worries about data sharing with Facebook and other parties that would go against the ideas of purpose limitation and data localization. Proactively, the Competition Commission of India (CCI) has opened an investigation into WhatsApp's controversial terms of service and privacy policy. The Competition Act of 2002 may have been broken, according to the CCI's inquiry. This is especially true with regard to WhatsApp's sharing of user data with Facebook and its affiliates. There has also been criticism of the policy's mandatory and non-negotiable character, which leaves users with no other option than to accept it or reject it.

In India, the courts have upheld the right to privacy in the wake of the K.S. Puttaswamy ruling. Limited legal redress is available under the current privacy framework, which is principally governed by Section 43A of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The proposed Personal Data Protection Bill, 2019 is proof that efforts are being made to pass comprehensive data protection laws. The 2019 Bill offers more comprehensive coverage than the current regime, with provisions that define personal data, guarantee user rights to access and erase their data, create explicit consent procedures and privacy notices, restrict data transfer outside of India, and require the appointment of a data protection officer.

People would have legal channels to report infringements on their private rights, and WhatsApp would have to abide by state laws under such legislation.

Because data protection laws exist in California, Brazil, and Europe, it is significant that WhatsApp has released distinct updated privacy policies for these users. However, India lacks strong data privacy laws, which exposes individual rights and fuels complicated legal issues. Consequently, the right to privacy is not

meaningfully enforced in the absence of data protection laws.

Analysis

The rights pertaining to abortion, prevention of unjustifiable abortion, and prohibition of female foeticide have been partially addressed in legislation across all three countries. For instance, India's Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994, touches upon these issues. However, there is a notable absence of legislation specifically regulating a woman's autonomy to decide on motherhood. The matter of abortion for women is considered a private affair. J. Nariman suggests that the right to abort should be classified among a host of private concerns. In India, a woman's right to abortion is contingent upon certain conditions. For instance, she must seek medical counsel before proceeding with an abortion if she is 12 weeks pregnant. Moreover, the Act prohibits a married woman from obtaining an abortion if she is not prepared to bear a child, even in cases where she may have been raped by her husband, thus restricting her freedom. Under these circumstances, a married woman lacks legal recourse.

In addressing data or information privacy, the Privacy Act of 1974 in the United States, the Data Protection Act of 1998 in the United Kingdom, and India's Information Technology Act of 2000 offer significant provisions.

A comparative examination of the facets, dimensions, and contemporary debates surrounding the Right to Privacy leads to the conclusion that the United States ranks highest in privacy protection, followed by the United Kingdom, with India still in the nascent stages of such safeguarding. Through judicial evolution, the preservation of privacy in matrimonial proceedings via in camera sessions has been established as a legal concept in the United States and the United Kingdom. Similarly, this provision is enshrined in marital legislation in India, including the Hindu Marriage Act of 1955, the Special Marriage Act of 1954, and the Divorce Act of 1869.

Constitutionally, the protection of the right to privacy is akin in the United States and India, as neither country explicitly guarantees this right in their constitutions, with its recognition solely a product of judicial interpretation. Conversely, the absence of a codified constitution in the United Kingdom has rendered its judiciary hesitant to acknowledge this right. In India, privacy has been shaped as a Customary Right in the rules of house construction, while in the United States, it has evolved as an inherent principle. Legislation in the United Kingdom remains relatively silent on the matter.

Conclusion

Attempting to confine the Comparative Analysis of Privacy Protection Laws to a specific framework proves futile, given the multifaceted nature of the Right to Privacy, which continues to expand over time. Consequently, the imperative for legislative safeguards for privacy rights is on the rise. A mere component-by-component comparison study falls short in drawing definitive conclusions. However, it is noteworthy that while ancient Indian laws once held significant superiority over Western counterparts, the contemporary landscape sees the United States emerge as the foremost jurisdiction in this regard. Meanwhile, the United Kingdom remains in the nascent stages of developing such laws.

Central to all these legal frameworks is their emphasis on data protection. In the era of information and communication technology, where the storage and processing of vast amounts of digital personal data are indispensable, the need for robust data protection measures is paramount for the survival of any nation.

REFERENCES

I. Case Laws – India

1. M.P. Sharma & Ors. v. Satish Chandra, District Magistrate, Delhi, AIR 1954 SC 300; 1954 SCR 1077.

2. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295; (1964) 1 SCR 332.
3. Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
4. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
5. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
6. State of Maharashtra v. Madhukar Narayan Mardikar, AIR 1991 SC 207.
7. Mr. X v. Hospital Z, AIR 1999 SC 495; (1998) 8 SCC 296.
8. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
9. Rayala M. Bhuvaneswari v. Nagaphanender Rayala, AIR 2008 AP 98.
10. R. Sridhar v. R. Sukanya, (2005) 1 MLJ 214 (Madras HC).
11. Jorawar Singh Mundy v. Union of India, W.P.(C) No. 3918/2020, Delhi High Court.

II. Case Laws – United States

12. Boyd v. United States, 116 U.S. 616 (1886).
13. Katz v. United States, 389 U.S. 347 (1967).
14. Smith v. Maryland, 442 U.S. 735 (1979).
15. Roe v. Wade, 410 U.S. 113 (1973).
16. Lawrence v. Texas, 539 U.S. 558 (2003).

III. Case Laws – United Kingdom & Europe

17. Goodwin v. United Kingdom, (2002) 35 EHRR 18 (ECtHR).
18. Google Spain SL v. Agencia Española de Protección de Datos, Case C-131/12, Court of Justice of the European Union (2014).

IV. Statutes & Legislative Instruments

India

19. Constitution of India, arts. 19, 21.
20. Information Technology Act, 2000, §§ 43A, 72A.
21. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
22. Right to Information Act, 2005, § 8(1)(j).
23. Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994.
24. Hindu Marriage Act, 1955.
25. Special Marriage Act, 1954.

United States

26. U.S. Constitution, amends. I, IV, V, IX, XIV.
27. Privacy Act of 1974, 5 U.S.C. § 552a.
28. Children's Online Privacy Protection Act, 1998.

United Kingdom

29. Human Rights Act, 1998, art. 8.
30. Data Protection Act, 1998 (UK).
31. Gender Recognition Act, 2004 (UK).

V. International Instruments

32. Universal Declaration of Human Rights, 1948, art. 12.
33. International Covenant on Civil and Political Rights, 1966, art. 17.
34. General Data Protection Regulation (EU) 2016/679.

VI. Scholarly Articles & Secondary Sources

35. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 **Harv. L. Rev.** 193 (1890).
36. J. Nariman, *Right to Privacy under the Indian Constitution*, (Commentary cited in judicial reasoning).
37. Justice B.N. Srikrishna Committee Report on Data Protection, 2018.