



Right To Privacy – A Study (Usa And India)

- UMANG
- AMITY UNIVERSITY
- LLM (HUMAN RIGHTS)

ABSTRACT

This paper provides a comparative analysis of the right to privacy in India and the United States, examining the legal and constitutional frameworks in both countries, and evaluating their alignment with international human rights standards, particularly those outlined in the Universal Declaration of Human Rights (UDHR). Privacy is recognized as a fundamental human right that safeguards personal liberties and protects individuals from unwarranted intrusion into their private lives. While both India and the U.S. offer legal protections for privacy through constitutional provisions and legislation, the scope and effectiveness of these protections vary significantly, especially in the digital age. In India, the right to privacy is enshrined under Article 21 of the Constitution, with landmark rulings like *Puttaswamy v. Union of India* (2017) affirming its fundamental status. Additionally, India is in the process of implementing the Personal Data Protection Bill to regulate data privacy. In contrast, the U.S. relies on the Fourth Amendment and sectoral laws like the Privacy Act and the Electronic Communications Privacy Act, but challenges remain, particularly concerning the balance between privacy and national security, especially in the post-9/11 context. The paper highlights key differences, such as the U.S.'s lack of comprehensive federal data protection laws compared to European standards, and India's struggle with surveillance programs like Aadhaar. Both countries face significant challenges in ensuring privacy in the digital era, where surveillance, data breaches, and technological advancements complicate privacy protection. The paper concludes by proposing stronger privacy regulations, better oversight of surveillance activities, and enhanced international cooperation to address the global nature of data flows and privacy concerns in the digital age.

INTRODUCTION

Privacy is a fundamental right afforded to all members of humanity, which pertains not only an essential characteristic of contemporary social fabric that protects personal liberties and rights. It means safeguarding privacy rights (like control over one's personal data and the right to be secure from unwarranted state or other incursion into his/her private life). Primarily privacy is important because it gives people space to develop who they are, understand how to create meaningful relationships and choose what kind of person (what combination of love/fear/hope/intellect/value/reasoning) want them or others ideally to be. This form of privacy, as a basic human right is even internationally recognized by the UDHR (The Rights Declaration), that protect individuals from random interventions.¹

It is an attempt to provide a comparative study of privacy rights in India and the United States, other aspects included are building on where they lie starkly with respect to protecting such right — branches. It also aims to determine if these protections comply with international human rights norms, specifically the standards established under the UDHR. The purpose is to generate an overview of the privacy regime in both nations — their legal and constitutional guarantees, but also challenges in light of contemporary technology trends.²

RESEARCH QUESTIONS

The research will provide answers to a few significant questions: How does the right of privacy work in India and United States? How well do these protections fit international human rights standards, such as the UDHR? The paper will answer these questions by examining the current status of privacy rights in both countries and discussing areas for potential reform.³

II. The Right to Privacy in International Human Rights Law

Privacy is a fundamental right afforded to all members of humanity, which pertains not only an essential characteristic of contemporary social fabric that protects personal liberties and rights. It means safeguarding

¹ Rajagopal, K. (2017, August 24). **Privacy is a fundamental right, declares SC.** *The Hindu*.

<https://www.thehindu.com/news/national/privacy-is-a-fundamental-right-declares-sc/article19551224.ece>

² U.S. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974).

³ United Nations. (1948). **Universal Declaration of Human Rights.** <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

privacy rights (like control over one's personal data and the right to be secure from unwarranted state or other incursion into his/her private life). Primarily privacy is important because it gives people space to develop who they are, understand how to create meaningful relationships and choose what kind of person (what combination of love/fear/hope/intellect/value/reasoning) want them or others ideally to be. This form of privacy, as a basic human right is even internationally recognized by the UDHR (The Rights Declaration), that protect individuals from random interventions.⁴

It is an attempt to provide a comparative study of privacy rights in India and the United States, other aspects included are building on where they lie starkly with respect to protecting such right — branches. It also aims to determine if these protections comply with international human rights norms, specifically the standards established under the UDHR. The purpose is to generate an overview of the privacy regime in both nations — their legal and constitutional guarantees, but also challenges in light of contemporary technology trends.

The research will provide answers to a few significant questions: How does the right of privacy work in India and United States? How well do these protections fit international human rights standards, such as the UDHR? The paper will answer these questions by examining the current status of privacy rights in both countries and discussing areas for potential reform.⁵

III. Right to Privacy in India

The right to privacy is derived from the Constitution of India, and in particular Article 21 which guarantees protection of life and personal liberty. While the Indian Constitution did not include privacy as a fundamental right at first, Indian jurists and judges have read it into Article 21 in an expansive manner. This settled interpretation that bore fruits in the seminal *Puttaswamy v. Union of India* (2017) decision, where a unanimous supreme court judgment stated unambiguously that there is an intrinsic or inherent part as envisioned-a right to privacy enshrined within fundamental rights embodied under Article 21 i.e., protection of life and personal liberty.. This ruling was important in the context of Indian constitutional law

⁴ General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council (2016).

⁵⁵ Solove, D. J., & Schwartz, P. M. (2020). **Privacy Law Fundamentals** (5th ed.). International Association of Privacy Professionals.

as for first time it evolved a jurisprudence on right to privacy being fundamental and its connotation with human dignity and autonomy.⁶

Apart from the constitutional protections, India has taken steps to buttress privacy rights under legislation. In the digital era, The Personal Data Protection Bill has been an essential initiative that paved way for extensive legal framework to save personal data. protect the not so anonymous timings of one trollshabit,. The fine-print of the bill has changed several times, but at its core it is intended to basically just regulate how data about you gets collected, stored and used- so that private companies stop using your information without permission or/and some douchey 3rd party (ahem Cambridge Analytica) steers elections with all this info. Also, the Indian judiciary is proving to be a mighty institution in securing privacy by intervening (as always) on snooping/data breaches/ other kinds of privacy violations that only makes sovereign legal framework more robust for people's freedom from surveillance.

However, in the face of growing surveillance and the rise of digital technologies, securing privacy safeguards remains a significant challenge for India. Serious questions have been raised as to whether or not existing safeguards are sufficient, especially given the potential for abuse by both government and private sector entities in snooping on almost all aspects of our digital lives. Moreover, finding the proper balance between privacy and national security as well as public interest continues to represent a challenge. Governments sometimes have to strike a balance between the collective rights of security and individual right to privacy in its surveillance initiatives for national safety measures. The reality is that this imbroglio continues to highlight the need for better laws and further regulatory safeguards surrounded by privacy while addressing real issues around security.⁷

IV. Right to Privacy in the United States

In the US, privacy is largely protected space built upon constitutional rights – namely through protections like those enshrined in our Fourth Amendment-bar not being subjected to government searches or seizures,. The Fourth Amendment, which limits the power of the government in personal and private affairs — property, communications and other aspects including data pertinent to personhood. The U.S. Supreme Court has offered further interpretation of the value of privacy in landmark decisions over time, as well. Every single one of these cases, starting with *Katz v. us* (1967), recognizes that people do have a "reasonable

⁶ Rubinstein, I. S., & Good, N. (2021). **Big data analytics: Privacy and the need for transparency.** *International Data Privacy Law*, 11(3), 202-215. <https://doi.org/10.1093/idpl/ipaa022>

⁷ *Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012 (India Supreme Court, 2017).

expectation of privacy," even in public places, thereby greatly limiting what can be done to them through the Fourth Amendment's protection for citizens 'privacy rights hampered costs introduced by Taney and his successors.currentTimeMillis And some, like Roe v. Wade (1973), may be primarily about abortion rights but still serve to enshrine a more general concept of personal privacy in our most intimate affairs. And in the digital age, just a few years ago this idea was cited again.. Carpenter v United States (2018) where Court held that mobile phone location information could not be accessed without warrant from government on historical basis which proved once more how privacy is much needed even in recent technological era as well.⁸

The U.S. privacy regime is further strengthened by a comprehensive body of legislative and regulatory laws, in addition to constitutional safeguards. One of the first few federal laws to address personal information collected by government agencies is The Privacy Act of 1974. Years later, in 1986, the Electronic Communications Privacy Act (ECPA) was established to include a provision for protecting digitally-communicated messages, including emails and telephone conversations among others although it has been criticized as being outdated due to fast-paced digital environment. Although the United States has not adopted legislation on data protection with a scope similar to that of European Union's General Data Protection Regulation ("GDPR"), there are several sectoral and state regulations modeled after GDPR principles, such as the California Consumer Privacy Act (CCPA), which is intended to protect individual rights over their own personal information in commercial transactions.

But the U.S. has been unable to get this right, as attempts at doing so have long clashed with issues surrounding privacy — particularly when such clash begin bleeding into national security interests. After 9/11, many Americans and others around the world have become very concerned with privacy loss as a fundamental right in order to be secure from terrorist threats by governments somewhat unchecked access under laws such as The Patriot Act. To this day, the debate on balancing national security with individual privacy continues to dominate due, in part, to post-9/11 surveillance programs and expanding data-gathering by intelligence agencies. Tech and data protection have added a layer of complexity to the digital era, as companies gather a wealth of personal info from users at all levels with little transparency or control for consumers. The landscape is rapidly changing and will only be more dynamic with the advance of new technologies as well as advancing digitisation around personal data, meaning that we must continually reassess how privacy can best be protected.⁹

⁸ Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848.

⁹ Roe v. Wade, 410 U.S. 113 (1973). United Nations. (1948). **Universal Declaration of Human Rights.**

<https://www.un.org/en/about-us/universal-declaration-of-human-rights>

V. Comparative Analysis: India vs. the US

The incursion of globalisation and technology into privacy rights in the digital age has been profound in both Australia and the UK. The ease in spread of information by digital technology is growing at a pace that India and America need to adapt quickly as they both have major concerns with respect to surveillance, social media and data protection. In a country as massive and broken, with large-scale surveillance programs in force we ding worry about more privacy being sacrificed at the alter of security resulting frombiometric data collection through schemes such as Aadhaar. In The USA, post-9/11 laws allow government surveillance and tech monopolies gather information on their users for profit. Predictable privacy is a dream in today's time of ongoing data breaches — with 02 Said that even offering the false promise makes us worse off than we already are! There were concerns about how personal data is exposed to security risks and unauthorised practice for both countries, especially on social media platforms. They highlight the urgent necessity for stronger regulatory frameworks in both countries that can combine privacy and technology.¹⁰

While both India and the U.S. offer domestic remedies to privacy, they fall short of Article 12 protections under UDHR since which has a constitutional implicit right to restrain any arbitrary interference with their personal livesPrivacy is not just left for human intervention but codified into law in constitution itself (Article 21). Although both countries provide for privacy in their constitutions or laws, the protection could be enhanced and more consistent with human rights standards. India is still in the process of refining its legal framework for data laws and regulations for privacy regulation need a more joined-up federal answer. Better privacy laws in both nations would recognize the fast-evolving landscape of digital data protection, remain vigilant about any surveillance gaps that arise and empower citizens to control what is done with their personal information.¹¹

VI. Challenges to Privacy in the Modern World

Over the course of this 21st century these norms have been reshaped by technological advancement (big data, AI & surveillance). Such technologies permit the enormous harvesting and analysis of personal information, providing a foundation for targeted advertising (the thing that makes so much online free), predictive analytics, you name it. Still, the broad reach of these technologies has brought about real fears in terms if data privacy as more and more details concerning individual persons risk being shared for potentially wrong reasons with private interests or governments. As a result, regulating the industry and protecting personal

¹⁰ Katz v. United States, 389 U.S. 347 (1967).

¹¹ International Covenant on Civil and Political Rights (ICCPR), United Nations, 1966.

data have encountered immense legal hurdles when odds are that various laws may not be capable of curtailing advanced technological advancements in this regard. A number of tech companies operate in multiple countries, which makes it harder to enforce data protection laws and comply with privacy regulations.

The Elrod — Harless decision maintained the contest between national security and individual privacy rights near the heart of any contemporary debate about privacy. Governments usually defend reducing privacy as a way to fight terrorism, cyber crime and other global threats for example. The Question of Privacy (or, Giving Up Some for National Security) Yes, we should be allowed to wear our underwear in private and not have the government come into our homes and look make sure no Muslim is teaching out children violent jihad. The tension between security and privacy has given rise to a sustained debate about the boundaries of state surveillance, as well as what protections should be afforded to citizens in terms of their own privacy. The problem is to strike the right balance between privacy and security, in a world that gains more threats of planetary proportions hiding behind bits every day.

Verifying that assertion, Special Rapporteur Heyns declared: What is clear from the Snowden Prism revelations in June 2013 and related events through into early 2014, discussed further below, on which this report also touches — summarizing detailed responses received to date from Governments of every continent as set out by region at the start — is beyond argument. The task is to avoid the infringement of privacy at all costs, while still having a secure world where people can own their data in an ever-growing network society.

VII. CONCLUSION

Therefore, the study has covered a comparative analysis of privacy rights in India and U.S., marking both similarities as well differences from legal backing way. They also provide the legal right to privacy in personal lives, and these are well scattered across courts for example The Puttaswamy judgement of India and Fourth Amendment of US. But while both provide the protection of law, there are some significant differences in how they protect data and regulate technology. From a comparative perspective against the Universal Declaration of Human Rights (UDHR), Article 12 and its components are well aligned in both countries, however complexities still persist with respect to achieving privacy protections without disruption by todays challenges such as surveillance or technological advancements.

It concludes with proposals for policy to improve the level of privacy protection in both countries, such as better data protection rules and more comprehensive federal framework needed especially in U.S. India to proceed with its Personal Data Protection Bill sharpening existing flaws. Both nations could also profit from greater oversight of surveillance activities and further restrictions that prevent national security policy from encroaching on privacy rights to an unwarranted degree. Enhanced international cooperation is required globally to deal with cross-border privacy challenges, as the technology companies and data flows are global.

The development of new technologies threatens to have a broader impact on privacy rights and could be the subject of future research, such as artificial intelligence, blockchain or biometric. More research is needed on how changing digital environments and heightened governmental surveillance are stretching conventional privacy boundaries, requiring legal reforms to better protect individual control over personal data in the information age.

