A COMPARATIVE EXAMINATION OF PRIVACY JURISPRUDENCE: INDIA AND THE USA

MR. SAURABH RAJ[1*], MR. PRATEEK SIKCHI[2] MR. SIDDHARTH RANKA[3]
[* 1,2, 3]Assistant Professor, Symbiosis Law School Nagpur, Symbiosis International (Deemed University), Pune Maharashtra, India
[*]Email: saurabhraj@slsnagpur.edu.in

Abstract

The right to privacy is judicially recognized as a fundamental right in India and the USA. In India and the USA, 'national security' is a ground that can be used to curtail the right of privacy. The paper analyzes the extent up to which this right to privacy can be legitimately inhibited on various other grounds and whether it can be violated by non-state actors.
The paper also analyzes the interference by the state in protecting the right to privacy. In the USA, the right to privacy is protected through certain sector-specific legislation as there is no comprehensive Act that protects this right. The paper also analyzes whether that approach can be applied in India with modifications as required.

Keywords: *Right to Privacy, Personal Data Protection Bill, ICCPR, State Action Doctrine*

Table of Contents

INTRODUCTION

Justice L. Brandeis of the U.S. SC defined the rights pertaining to privacy as "the most comprehensive of rights and the right most valued by civilized man".[1]

Many countries of the world expressly provide for the right to privacy under their constitutions for instance, in the newly written Constitution of the South Africa the right to access and control personal information is granted. However, in some countries, the Right to Privacy is not expressly recognized and that is interpreted under one or the other provision in the Constitution itself. The right to privacy is available to citizens in many countries, however, the standard of protection varies. The right to privacy has changed throughout time, and this change may be observed via a succession of court decisions.

The Supreme Court of India's decision in the case of M.P. Sharma v. Satish Chandra[2] was the first step on the path towards the recognition of the right to privacy in India. However, a limited right to privacy was recognised in Kharak Singh v. State of Uttar Pradesh[3] with regard to private residences but not to public spaces.

[1] Olmstead v. United States, 277 U.S. 438, 478 (1928).
[2] M.P. Sharma v. Satish Chandra, (1954) SCR 1077.
[3]Kharak Singh v. State of Uttar Pradesh, (1954) SCR 1077.

Furthermore, the Supreme Court declared in Gobind v. State of M.P.[4] that privacy is protected by Article 21 of the Indian Constitution since it is closely related to and overlaps with the notion of liberty. The state cannot force its citizens to disclose or reveal the material to the public, as was ruled in Ram Jethmalani v. Union of India[5]. This is because the right to privacy is an intrinsic part of the right to life. Disclosure of this kind should only occur under proper and acceptable circumstances. This issue has been resolved once and for all.

The Indian Supreme Court has widened the applicability of basic rights guaranteed by the Indian constitution, making them legally binding against the Indian government. The issue at hand is whether or not a claim for privacy may be made against organisations that are not part of a state.

Informational privacy is the focus of this paper, but there are other types of privacy as well, including physical privacy, which Justice Cooley defines as "the right of a person to be let alone," and privacy as to choice, which means an individual's right to do things of his own choice without interference from the outside. The concept of "informational privacy" refers to how privately or publicly identifiable information is handled and shared. Specifically, whose information is it, anyway? Can I ask who has access to this information? To what degree are these records available for commercial and government use?

Specifically, the article will compare and contrast the Right to Privacy in India and the United States. In India, the right to privacy is qualified rather than absolute, meaning that it may be limited provided the government can show that they have a compelling reason to do so and have satisfied three other criteria. The first criteria is whether or not there is a legislation in place. Article 21 further ensures that no part of an individual's life or freedom may be taken away without due process. As a result, restricting the right to privacy requires a constitutionally sound regulation.

Second, there must be a legitimate governmental objective that safeguards the right against arbitrary acts on the part of the State. Finally, there must be a reasonable link between the goals and the methods to attain them in order to pass the proportionality test.

In several decisions, the Supreme Court of the United States has upheld the existence of a constitutional right to privacy in the United States. The right to privacy, which is otherwise recognised by multiple amendments to the U.S. Constitution, was given explicit Constitutional standing in Griswold v. Connecticut.

It's important to remember that as technology evolves, so does the medium of privacy. As a result, the concept of "Informational Privacy" came into being. When the government or private organisations collect and store information on everyone and everything, protecting people's privacy becomes more difficult.

The laws of the United States, both their protection level and their manner of protection, must be understood in order to govern this informational privacy. We will next compare and contrast how India and the United States handle data privacy.

Justice Chandrachud in the Puttaswamy case[6] said, "Informational privacy is a component of the right to privacy. In this digital era, threats to privacy are not limited to those posed by the state. Building such a system demands consideration of both private interests and the state's legitimate needs.

Patient or medical record privacy is a subset of the broader data privacy problem. The right to privacy and other rules and regulations help ensure that people may exercise this freedom. There is an effort underway by the government to strengthen protections for the right to privacy in all its forms. Attempts at regulating this kind of data handling include the proposed Personal Data Protection Bill of 2018, the Digital Information Security in Healthcare Bill of 2018, and others. Similar thinking can be observed in the United States, where the HIPAA Act and the subsequent HITECH Act have both been passed. As we examine this matter, we shall do so through the lens of the relevant sections of these

[4] Gobind v. State of M.P., (1964) 1 SCR 332.

[5] Ram Jethmalani v. Union of India (2011) 1 SCC 711.

[6] Justice KS Puttaswamy (Ret'd) v. Union of India, (2017) 10 SCC 1.

statutes.

1. CONCEPT & EVOLUTION OF PRIVACY

Having a safe space to call one's own is a basic human need that carries extra weight in today's world. This privilege has been around for a very long time. It means no one can intrude on a person's life without that person's permission and no one can force them to do anything they don't want to.

Although privacy is not explicitly guaranteed by Indian law, it is increasingly being acknowledged throughout the country. By interpreting Article 21 broadly, the Indian Judiciary has broadened the scope of privacy protections. Article 21's protection of "personal liberty" adequately acknowledges the right to privacy.

The Latin word privatus, from which we get the word "privacy," implies "to shut off the world." Because of this subjectivity, the concept of privacy is difficult to define. The concept of personal space developed with the idea of independence. John Locke argued that the right to one's own privacy was essential to the concept of individual liberty. To have privacy is to have a place of one's own where one may relax and let his guard down.

The principle of privacy protection is ingrained in some laws. The Indian Telegraph Act of 1885 is one such law; it states that the state may interfere with communications in the event of a public emergency but not otherwise. So, the Act also included protections for personal information.

In the landmark US case Simonsen v. Sewnson, it was determined that doctors have a professional and ethical obligation to protect their patients' privacy and any sensitive information they may obtain while acting in their professional capacity. However, disclosure may occur if it is in the patient's or the public's best interest, or if disclosure is authorised by law. In a similar vein, material may be revealed in India if it is in the state's "compelling interest."

In the United States, the right to privacy in making decisions has been upheld in several judgements. Individuals' autonomy in making choices about their bodies and families was upheld as a right in the case Griswold v. Connecticut.[7] Although this right is not explicitly mentioned, it is guaranteed by the Bill of Rights and other amendments to the US Constitution.

Similarly, the Supreme Court's decision in Whalen v. Roe[8] upholds the right to privacy in one's personal information. A person's right to keep private information to themselves is included under the concept of "informational privacy." Nixon v. Administrator of General Sciences also made reference to this interest. In light of these instances, several US circuit courts now acknowledge the importance of protecting individuals' right to privacy with regard to their personal information.

U.S. citizens' right to privacy is safeguarded not by any provision of the Constitution but by later amendments. The broad right to privacy, including the right to protection of property, life, etc., is the duty of the states, however there are provisions in the US Constitution which safeguard the private of individuals from the intrusion of the state.

The Supreme Court of the United States acknowledged in the case of Jane Roe v. Henry Wade[9] that the right to privacy is not explicitly stated in the Constitution. The Opening, Fourth, Fifth, and Ninth Amendments laid the groundwork for this right, and the notion of liberty is mentioned in the first part of the Fourteenth Amendment.

It's worth noting that the U.S. Constitution only guarantees a "qualified" right to privacy. The case of Olmstead v. United States established that an individual's expectation of privacy may be limited or ignored if the state has a more important interest. There must be justification for the state to step in.

2. DATA PRIVACY AND MEDICAL INFORMATION

"an individual's claim to control the conditions under which personal information, i.e., information

[7] Griswold v. Connecticut, 381 U.S. 479 (1965).
[8] Whalen v. Roe, 433 U.S. 425 (1977).
[9] Jane Roe v. Henry Wade (1973) 410 US 113.

identifiable to the individual, is collected, released, and utilised," as defined by the US-based IITF principles, is what we mean when we talk about information privacy. In this context, "data privacy" refers to the interplay between data collection and distribution, as well as the associated technological, legal, and political concerns.

INDIA

Ruling of the Supreme Court in the case of Justice K.S. Puttuswamy (Ret'd) & Anr. v. Union of India, often known as the privacy judgement, legally recognised the Right to Privacy in India. This decision cites the South African Court decision NM & Ors. v. Smith & Ors., in which the need of protecting patient privacy while handling medical information was stressed. It was decided there that medical records should be kept private since disclosure may compromise patients' wishes.

An Indian court has ruled that the unauthorised disclosure of medical history is an invasion of privacy and, thus, a violation of basic rights. It is appropriate for the government to request this information from hospitals in certain cases, such as when doing disease or pandemic analysis.

AN INDIAN ATTEMPT AT LEGISLATION

Privacy of data has been a major concern in the wake of the privacy verdict, and the government has made some efforts to prevent the misuse of sensitive health information. The Digital Information Security in Healthcare Data Protection Bill, 2018 (hence referred to as DISHA) is one such effort aimed at safeguarding Indian individuals' digital health data. The Digital Information Security and Privacy Act of 2015 (DISHA) and the Personal Data Protection Bill, 2019 will provide a safe haven for digital health records and prevent their disclosure. Massive and very sensitive, health data is collected and stored by hospitals, clinics, etc.

Information is now safeguarded by the Information Technology Act of 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011. The Act and the rules provide that the data must be safeguarded and that, in the event of a breach being notified, compensation must be granted. Even sensitive personal data may be gathered by government agencies without prior authorization, so long as it is collected for a specific reason and that purpose is communicated to the individual being monitored.

It's important to remember that things work somewhat, but they don't solve every problem. In cases of data breaches, patients will not be notified; only sensitive data that is created or sent electronically will be safeguarded.

The Data Integrity and Privacy Shield Act (DISHA) is joined by the Personal Data Protection Bill (PDP Bill) of 2019. Health data, as defined in section 3(21) of the PDP Bill, is information on a data principal's physical or mental health. In accordance with the PDP Bill's definition of "sensitive personal data" in section 3(36), the health records fall into this category. At the outset of any processing of the data principle's sensitive personal data, the data principal must provide their express permission. In accordance with DISHA, every organisation that is neither a clinical facility or a health information exchange is required to get explicit permission before collecting any personally identifiable information.

As part of its National Digital health initiative, the government has released a draught of the Health Data Management Policy. This document details the procedures to be followed in collecting, processing, and storing patient data (NDHM). The mission's execution will fall within the purview of the National Health Authority.

The user's capacity to withdraw consent at any time is a crucial feature of this ID. According to the rules, all parties involved in the processing of the data (including, but not limited to, health information providers and health information consumers) must establish procedures for handling any unauthorised access to sensitive information.

Using this system, any breaches in the protection of patient information may be quickly identified and reported to the National Health Authority. The purpose of this plan is to improve current methods of safeguarding individuals' right to privacy with regards to their medical records.

The analysis of the legal perspective on privacy is essential to the study of the Right to privacy. It was ruled in the case of Neera Mathur v. Life Insurance Corporation[10] that Ms. Mathur was obligated to provide private information about her conceiving, pregnancy, menstrual cycles, etc., to the LIC upon joining the LIC.

United States of America

Data is particularly susceptible to abuse in the hands of state actors owing to the absence of remedies against them, hence it is essential that individuals' data be safeguarded from them. The Bill of Rights in the Constitution provides several safeguards against governmental encroachment on personal privacy, but offers fewer avenues for redress against private actors. The Fourth Amendment guarantees citizens the "right to be secure in their persons, homes, documents, and effects, against arbitrary searches and seizures," among other protections for personal privacy.

The Fourth Amendment was formerly understood to represent little more than a restriction on government intrusion into people's homes, but over the years it has come to be construed in a way that also guarantees a broad right to privacy across the United States. Constitutional principles have progressed in tandem with the common law, and the right to privacy has received the recognition and protection it deserves.

In the decision of Katz v. United States[11], the Supreme Court of the United States declared that individuals, not just locations, are protected by the Fourth Amendment.

Digital privacy is an extension of this notion that ensures data is safeguarded across online platforms. The Supreme Court of the United States recently declared in Carpenter v. United States that the Fourth Amendment protects citizens' right to privacy, even when government agencies disclose otherwise public information to private entities. It is fair to anticipate that mobile phone carriers would respect the privacy of their customers' location and movement data, and the Fourth Amendment guarantees this right. The Supreme Court of the United States differentiated the approaches employed in United States v. Miller[12] and Smith v. Maryland[13] in the Carpenter case. The Supreme Court ruled in the Miller and Maryland instances that Fourth Amendment protections do not apply to material that has been disclosed to third parties. The aforementioned incidents include violations of the Fourth Amendment's protections against unlawful search and seizure. The Carpenter decision mandates that the government must demonstrate a need for information from third parties in order to be granted a warrant. In the area of digital privacy, the Fourth Amendment established a limited protection against the unwarranted intrusion by governmental agencies.

The right to privacy was expanded in the Fourteenth Amendment, which is why it's crucial to remember that the word "liberty" is included in the amendment. This amendment safeguards against governmental overreach other than search and seizure.

The US Supreme Court's decision in Whalen v. Roe established that the right to privacy guaranteed by the Constitution protects two distinct types of interests. First, it's about having control over your own data and how you share it, and second, it's about having complete discretion over certain life choices.

The first of them is the "right to informational privacy," which entails the safeguarding of personal information. After the decision of Whalen v. Roe, the Supreme Court broadly expressed the right to privacy, yet subsequently sustained government initiatives that were argued to violate individuals' privacy.

The Court here held that disclosure requirements are "essential to current medical practise," and that legal protections exist to prevent the unwarranted release of private information. That's why the court upheld the New York law.

Uncertainty persisted as to the Supreme Court's stance on informational privacy, although the

[10] Neera Mathur v. Life Insurance Corporation, AIR 1992 SC 392.
[11] Katz v. United States, 389 U.S. 347 (1967).
[12] United States v. Miller, 425 U.S. 435, 443 (1976).
[13] Smith v. Maryland, 442 U.S. 735, 741 (1979).

overwhelming majority of federal circuit courts accepted the right in some capacity.

Information privacy is still a taboo topic because of this. Concerns about data collection, storage, and usage all fall within the purview of the right to privacy.

The state action doctrine' holds that individuals have a right to privacy solely with respect to state activity and not in any context outside of state action. This is why the Right to privacy does not include completely private activities. The right to privacy may also be violated by private actors, and it is not possible to bar them using the right to privacy alone.

Therefore, the right to privacy and data theft is not fully protected by constitutional provisions and common law rights. Therefore, the most important guidelines for data security may be found in statute.

The United States lacks a general legislation protecting individuals' privacy. However, the company's privacy practises and data use are governed by federal and state legislation. This legislation extends the right to privacy guaranteed by the US Constitution to non-government organisations. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a key piece of US law to keep in mind here since it establishes and safeguards a category of medical data known as "protected health information" (PHI). It's the first law at the federal level specifically addressing health information privacy.

All businesses that provide medical services may take use of HIPAA's standardised structure. Entities, Health Care Providers, Health Plans, and Health Care Clearinghouses are all included, along with their respective business connections. The HIPAA regulates a wide range of privacy-related problems, including the use or disclosure of protected health information (PHI), the disclosure of information, the security measures that must be taken to safeguard PHI, etc.

3. ISSUES & CHALLENGES

In the doctor-patient interaction, it is the patient's responsibility to provide relevant medical history details in order to get effective care and prevent unwanted medication side effects. Patients may be reluctant to disclose some facts, such as the presence of an HIV infection or a mental health issue, for example, owing to the societal stigma that surrounds these conditions. Over time, this data builds into a complete record that no outsiders should be able to see. The patient's treatment history, medical diagnoses, sexual orientation, past jobs, family medical history, genetic information, etc.

A key question is whether or not private information may be coerced to be disclosed to non-state parties. Since no limitation exists that prevents Article 21 from being applied to private parties, the right to privacy may be extended to non-state actors as a solution to this problem.

Digitization of medical files has given rise to new security risks. There are a number of risks that make the protection of personal data essential. The following are some of the dangers:

1: Dangers to the Organization

2) Systemic Dangers

Organizational risks include those posed by employees who get unauthorised access to data or who violate the limits of their permitted access. These dangers to the organisation may be broken down into five groups:

First, there's accidental disclosure, which occurs when sensitive patient information is sent to the incorrect e-mail address or shared in some other way without the patient's knowledge or consent.

Second, it's not uncommon for employees with access to patients' private information to utilise it for their own purposes or out of pure curiosity. Furthermore, celebrity information is particularly vulnerable to such leaks.

It has also been noted that insiders connected with hospitals or clinics that store sensitive information participate in obtaining and sharing the data for financial or other gain.

Fourth, unauthorised access to data (also known as a "data breach") occurs when an outsider obtains access to an organization's private information via illegal means. They break into secure buildings (hospitals, government offices, etc.) by force and steal sensitive information.

Fifth, intrusion into a network system is a common danger because of technical advancements. Former workers, hackers, or anybody else with an interest in such data get unlawful access to the computer system and the data it contains.

INDIA

It was held in the case of Tokugha Yepthomi v. Apollo Hospital Enterprises Ltd.[14] that the Constitution's Fundamental Rights are qualified by reasonable constraints. The court ruled that the right to privacy must yield to the greater good, citing the cases of Kharak Singh v. State of U.P.[15], Munn v. Illinois[16], and Wolf v. Colorado[17]. It was also noted that regardless of the financial nature of the doctor-patient relationship, the doctor owes the patient a duty of secrecy.

While protecting patients' privacy calls for keeping their medical records under wraps, disclosure should be permitted for the greater benefit when there are strong reasons and justifications to do so.

The husband in Sharda v. Dharmpal[18] claimed that his wife's mental illness justified a divorce. She claims that a medical examination, required to show mental disorder, violates her right to privacy and liberty.

The Central Information Commission ruled in the case of Shri G.R. Rawal v. Director General of Income Tax (Investigation)[19], which involved the RTI Act, that the Act's exemption for such information would not apply in situations where the disclosure of such information would serve a greater public interest. The Court upheld the disclosure of a prisoner's medical information in response to an RTI request, citing a Bombay High Court decision in the matter of Mr. Surup Singh Naik v. State of Maharashtra via Additional Secretary.

From the following decisions, it is clear that the right to privacy is often sacrificed for the greater public good. There is no consistent judicial stance on the issue of what constitutes the greater public interest, so each case must be decided individually. Due to this, people in India are losing their freedom, privacy, and independence at an alarming rate. Additionally, there is no right to be removed. The right to be forgotten refers to the option to restrict or update previously disclosed personal data. Problems arise when private information is transferred across international borders without proper safeguards and informed consent. To properly safeguard personal information, the proposed laws must address these concerns.

4. THE UNITED STATES

Seventy-five percent of American patients are worried that their personal information is being shared without their knowledge or consent by health websites, according to a recent poll. Proof of this may be seen in the fact that the exposure of medical information is the second most often reported breach. Several efforts, like as the HIPA Act, have been taken at the federal and state levels in the United States as a result of this violation of patients' right to privacy and disclosure of medical information.

A person's right to privacy in medical matters is guaranteed by both the Constitution and federal and state law. While HIPAA was intended to safeguard patients' personal health information, it is not without its restrictions. The first problem is that not every individual or organisation that deals with medical records is within the purview of the Act. HIPAA applies to the information kept by health care providers, clearinghouses, and insurance companies.

It is important to remember that HIPAA only applies to healthcare providers, hospitals, pharmacies,

[14] Tokugha Yepthomi v. Apollo Hospital Enterprises Ltd., AIR 1999 SC 495.
[15] Kharak Singh v. State of U.P., AIR 1963 SC 1295.
[16] Munn v. Illinois, (1877) 94 US 113.
[17] Wolf v. Colorado, (1949) 338 US 25.
[18] Sharda v. Dharmpal, AIR 2003 SC 3450.
[19] Shri G.R. Rawal v. Director General of Income Tax (Investigation), No. CIC/AT/A/2007/00490.

and health insurance companies; there are still certain third parties that have access to protected health information who are not covered by HIPAA. Many, many websites, for instance, gather medical data yet are not covered by HIPAA.

The second problem is the widespread usage of law enforcement access to patients' medical records. Without a warrant or subpoena, police enforcement may examine a person's medical records. Additionally, a suspect, fugitive, missing person, etc. may be identified or located with the help of a health record request.

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 addresses some of these concerns by, among other things, increasing the severity of fines for HIPAA violations and expanding the scope of HIPAA's enforcement to include business associates of covered entities that are recipients of protected health information. Also included is a notification system in the event of a medical data breach.

5. CONCLUSION AND SUGGESTION

Over time, the idea of privacy has changed in both India and the United States. Even while privacy isn't guaranteed by either the Indian or American constitutions, it may be found in decisions courts have made and laws that have been passed. The demand for privacy protection has grown with the spread of information and communication technologies in countries like India and the United States, prompting lawmakers in both countries to draught and explore new privacy laws. Before the advent of the internet, paper medical records were the norm, but nowadays everything is kept in digital form and can be accessed from anywhere in the globe.

Digital patient records, reports on diagnoses, illnesses seen, treatments administered, test results, appointment information, drugs bought, genetic data, sexual orientation, religious beliefs, and other personal information are just some of the types of data that may be found online. The data is shared across different organisations for many reasons, not only between hospitals and clinics. Information that a person wants to remain private is an accurate definition of privacy. Informational privacy is only one subset of the broader concept of privacy.

Databases have been created specifically for the purpose of storing and managing people' private information. In most cases, only the individual who generated the data should have access to it. Unfortunately, though, there is no way that could ever be done in practise. When people's personal details are stored in centralised databases, it may do serious harm to their informational privacy. It is important to remember that despite the right to privacy being formally recognised by the courts, it still requires protection via laws and other restrictions.

In today's world, India's present laws and regulations are insufficient, and the country will face much greater difficulties in the years to come. The gathering, sharing, leaking, and connecting of data, etc., are all sources of modern information privacy issues, especially in the context of medical information or records. The Indian Parliament has taken action in this direction by passing the Data Protection law, 2019, which, if passed, would settle many outstanding concerns. The DISHA law, a specialised piece of legislation dealing with the subject of medical privacy, will do much to protect the confidentiality of patients' health information and to ensure that individuals' private rights are respected. Both of these legislation are urgently needed at this time.

Considering the sensitive nature of the data involved, the DISHA law should be limited to include only clinical facilities and health information exchanges. Personal Data Protection Bill, 2019 may be used to regulate other applications or wearable devices that provide M health services. If there was any potential tension between the PDP Bill and the DISHA Bill, this should help alleviate it.

The lack of a comprehensive law on data privacy is a major gap in the existing Indian legal system, as we learn from our examination of the right to privacy in relation to medical information.

Second, there is no organisation of the data into distinct categories, such as public, private, or sensitive.

The fact that no statute addresses the question of who owns personal and confidential records.

4. There is no foolproof system in place for generating, processing, transferring, or storing data.

5. The lack of regulations addressing the international exchange of health records.

In the United States, patients' medical records are safeguarded by federal and state regulations as well as constitutional provisions. Maintaining patients' confidentiality is essential to ensuring they are able to fully exercise their right to privacy. As we've seen, the HIPAA has several holes that need to be filled. The American judicial system is cited as another example of its complexity and technicality. The US government has taken a number of steps to ensure the privacy of its citizens' personal information, and it also protects some categories of personal information from public view. Because of this, there is a pressing need in the United States for a comprehensive law that can protect individuals' right to privacy and security of their personal information.

Administrative safeguard, technological safeguard, physical safeguard, etc. in India would assist define policy and method for protecting medical and health records' confidentiality. In the event that a patient's information is compromised or revealed without their permission, there must be a mechanism in place and an officer designated to carry it out. The policy should also specify which categories of personnel have access to patients' electronic records, and whether or not such access requires additional safeguards. When disclosing sensitive information, care must be taken to ensure that the recipient is who they claim to be.

BIBLIOGRAPHY

References:

National Collegiate Athletic Ass'n v. Tarkanian (1988) U.S. Supreme Court.
Solove, D. J., & Schwartz, P. M. (2020). Information Privacy Law [Connected eBook] (Aspen Casebook) (7th ed.). Aspen Publishing.
Global Litigator: A Litigatorâ□□s Primer on European Union and American Privacy Laws and Regulations. (n.d.). https://www.americanbar.org/groups/litigation/publications/litigation_journal/2017-18/winter/a-litigators-primer-european-union-and-american-privacy-laws-and-regulations/
Right to Privacy. (n.d.). Harvard Law Review.
Solove, D. J., & Schwartz, P. M. (2020). Information Privacy Law [Connected eBook] (Aspen Casebook) (7th ed.). Aspen Publishing.

ARTICLES

1. 3 Steven Lukes, "The Meanings of Individualism", Journal of the History of Ideas, (1971).
2. Applebaum, P.S., 'Privacy in psychiatric treatment: threats and response', American Journal of Psychiatry, Vol. 159 (2002).
3. Chatterjee Sangeeta & Bandyopadhyay Dr Rathin "Confidentiality of Information as Right to Privacy: A Comparative Analysis of Indian, U.S. and British Laws", India International Journal of Juridical Sciences, (Mar 2012).
4. Daniel J. Solove & Paul M. Schwartz, Information Privacy Law (5^{th} ed. 2015). 5. Daniel J. Solove & Paul M. Schwartz, Information Privacy Law (6th ed. 2018).
6. David H. Flaherty, On the Utility Of Constitutional Rights To Privacy And Data Protection (Case Western Reserve Law Review 1991).
7. Hasan, R. and Yurcik, W. (2006) 'A statistical analysis of disclosed storage security breaches', Proceedings of 2nd ACM Workshop on Storage Security and Survivability, Alexandria, VA.
8. Jeffery L. Johnson, "A Theory of the Nature and Value of Privacy", 6(3) Public Affairs Quarterly 271-288 (1992),
9. Leon A. Pastalan, "Privacy as a Behavioural Concept" 45(2) Social Science 94 (1970).
10. M G Michael & Katina Michael, Uberveillance and the social implications of microchip implants : emerging technologies, Hershey, PA, Information Science Refernce, p.3 (2014).
11. Mercuri, R.T. (2004) 'The HIPAA-potamus in health care data security', Communications of the ACM, Vol. 47, No. 7.
12. National Research Council, For the Record: Protecting Electronic Health Information, National Academy Press, Washington DC (1997).
13. Pew Internet & American Life Project, Institute for Healthcare Research And Policy, Georgetown University, exposed online: Why the New Federal Health Privacy Regulation Doesn't offer Much Protection to Internet users (Nov. 2011).
14. Raman, A. (2007) 'Enforcing privacy through security in remote patient monitoring ecosystems', 6th

International Special Topic Conference on Information Technology Applications in Biomedicine, Tokyo, Japan.
15. Samuel Warren and Louis Brandeis, "The Right to Privacy" 4 Harvard Law Rev. (1890).
16. Shivnath Tripathi, Right To Privacy As A Fundamental Right: Extent And Limitations (2017)
17. Vrinda Bhandari and Renuka Sane, Protecting Citizens From The State Post Puttaswamy: Analysing The Privacy Implications Of The Justice Srikrishna Committee Report And The Data Protection Bill, 2018 (2020)
18. Zachary S. Heck, A Litigator's Primer on European Union and American Privacy Laws and Regulations, 44 Litig. (2018).
CASES

FOREIGN CASES
16. Carpenter v. United States, 138 S. Ct. 2206 (2018).
17. Griswold v. Connecticut, 381 U.S. 479 (1965).
18. Jane Roe v. Henry Wade (1973) 410 US 113.
19. Katz v. United States, 389 U.S. 347 (1967).
20. Munn v. Illinois, (1877) 94 US 113.
21. NASA v. Nelson, 562 U.S. 134, 159 (2011).
22. National Collegiate Athletic Ass'n v. Tarkanian, 488 U.S. 179, 191 (1988). 23. Nixon v. Administrator of General Sciences, 433 U.S. 425 (1977). 24. NM & Ors. v. Smith & Ors., 2007 (5) SA 250 (CC).
25. Olmstead v. United States, (1927) 277 US 438 (471).
26. Simonsen v. Swenson, 177 N.W. 831 (Neb. 1920).
27. Smith v. Maryland, 442 U.S. 735, 741 (1979).
28. United States v. Miller, 425 U.S. 435, 443 (1976).
29. Whalen v. Roe, 433 U.S. 425 (1977).
30. Wolf v. Colorado, (1949) 338 US 25.

INDIAN CASES
11. Gobind v. State of M.P., (1964) 1 SCR 332.
12. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
13. Kharak Singh v. State of Uttar Pradesh, (1954) SCR 1077.
14. M.P. Sharma v. Satish Chandra, (1954) SCR 1077.
15. Mr. Surup Singh Naik v. State of Maharashtra through Additional Secretary, AIR 2007 Bom 121.
16. Neera Mathur v. Life Insurance Corporation, AIR 1992 SC 392. 17. Ram Jethmalani v. Union of India (2011) 1 SCC 711.
18. Sharda v. Dharmpal, AIR 2003 SC 3450.
19. Shri G.R. Rawal v. Director General of Income Tax (Investigation), No. CIC/AT/A/2007/00490.
20. Tokugha Yepthomi v. Apollo Hospital Enterprises Ltd., AIR 1999 SC 495.

LEGISLATIONS
1. Digital Information Security in Healthcare Bill, 2018.
2. Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A.
3. Health Insurance Portability and Accountability Act, 1996
4. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
5. Information Technology Act, No. 20, Acts of Parliament, 2000. 6. Right to Information Act, No. 22, Acts of Parliament, 2005.
7. The Constitution of India, 1950.
8. The Indian Telegraph Act, 1885.
9. The Personal Data Protection Bill, 2018.
10. The U.S. Constitution

MISCELLANEOUS
1. Information Infrastructure Task Force, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information ("IITF Principles") (1995).

WEBSITES
2. Asheeta Regidi, 'Right to Privacy Verdict: Is It Enforceable Against A Private Technology Company Such As Whatsapp? - India News, Firstpost' (Firstpost, 2020)
3. 'Health ID Data Privacy: Patients To Be Able To Withdraw Consent 'Any Time'' (The Indian Express, 2020)
4. India.com Desk, 'Amrita Arora Lashes Internet For Leaking Sister Malaika Arora's COVID-19 Report' (India News,

Breaking News, Entertainment News | India.com, 2020)
5. Jeevalaya. V, 'The Concept of Right to Privacy and Constitutional Validity Of AADHAAR' (Worldwidejournals.com, 2020)