E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 14-08-2023
Accepted: 30-09-2023

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 1; Issue 2; 2023; Page No. 549-553

Right to privacy in the modern digital age

[1]Pooja Rani and [2]Dr. Vivek Kumar Gupta

[1]Research Scholar, Sunrise University, Alwar, Rajasthan, India
[2]Professor, Sunrise University, Alwar, Rajasthan, India

DOI: https://doi.org/10.5281/zenodo.14947726

Corresponding Author: Pooja Rani

Abstract

Privacy is crucial for individuals to decide what personal information can be shared and with whom. As people's lives become more connected to digital platforms, protecting digital privacy becomes increasingly important. This analysis examines whether India's security and human rights legislation meets international standards. While Indian security regulations generally align with global norms, there are some outliers due to sloppy execution and political misuse. The government has begun manipulating free speech, with little assistance from "censoring," to create an image that aligns with their agendas. The concepts of "censorship" and "Right of freedom of expression" are on opposite sides of a spectrum, and the unjustified relaxation of censorship claims contradicts its own justifications. Censorship is a transnational phenomenon that impacts all nations equally, adapted by every administration to suit its social and cultural norms. The power battle between the Censor Board and the importance of free speech is a key issue. The constant data collection and processing in the market makes the right to privacy an increasingly pressing issue in this modern age. The advent of digitization has led to illegal practices such as data fraud, hoax contacting, and cyber harassment. Data acquisition, storage, monitoring, recording, access, processing, dissemination, and upkeep are not regulated by any national statute. Therefore, understanding and protecting digital privacy is essential for maintaining a healthy and inclusive society.

Keywords: Privacy, digital, freedoms, social media, human rights

Introduction

Respect for personal space is a major concern in every region of the globe. Humans have innate desires and ideals related to their social nature, and one of such fundamental rights is the right to privacy. A plethora of meanings is associated with privacy. On a daily basis, individuals, groups, and the state all make claims in a variety of contexts.

The term "privacy" refers to a person has many rights, such as the following: the right to think and speak freely, the freedom to move about as one pleases, the right to privacy at home, the right to control one's own data, the right to not be watched, the right to have one's reputation protected, and the right to be free from searches and interrogations. Privacy is a vague concept in and of itself. I don't think it's nebulous or difficult to pin down; rather, it's quite fluid, subject to shifts in the political and technical climate as well as the definitions of privacy and rights imposed by different regulatory bodies and governments throughout the globe.

In today's world, where the internet is always there, people's right to privacy is seen as having multiple dimensions. It's no longer just about physical privacy; it also encompasses communication and information privacy. The notion of privacy protection has taken on a multi-faceted nature in this digital era.

Having some say over who knows what about ourselves is fundamental to the concept of privacy. Privacy is especially important in the digital realm since so many choices are based on data and information. In order to safeguard our independence, to control what happens to us online, what we view online, and the choices that are made about us and for us, we need safeguards with the purpose of gathering, using, and preserving individual data.

The liberty of every person to privacy ensures that their private information is shielded from public view, therefore maintaining their dignity. Freedoms, both good and bad, are associated with privacy. The right of a person to privacy encapsulates their positive freedoms with respect to four main areas of law: the liberty to choose one's own path through life, the autonomy to control one's own data, the

ownership and upkeep of one's own property, and the freedom to have control over one's own physical space. Privacy, as a negative freedom, is defined as the non-invasion of one's personal space by other parties such as the state or corporations.

Literature Review

Rahul Matthan (2018) [2] discusses the personal space we have in books. The author follows the development of privacy concepts from their inception to the present day by analysing seminal instances across the US, India, and the UK but doing so, he reimagines how we should be thinking about privacy in the current day in order to make the most of data technologies, but also warning against becoming fixated on their possible downsides to the point where we create legislation that prevents us from utilising them.

From the standpoint of accessibility and readability, Rishab Bailey, Smriti Parsheera, In their 2018 evaluation, Faiza Rahman and Renuka Sane look at the privacy regulations of five well-known Indian internet providers. Questions such, "Do policies have specific, unambiguous, and clear provisions that lend themselves to easy comprehension?" and "How much do users typically understand of what they are signing up for?" were both attempted to have their answers found by the writers. According to the authors, the policies that were examined had weak wording and often seemed to be a means to a goal-the mere compliance with anticipated privacy disclosures. Policies with the fewest specifics and those that were too lengthy received the lowest response rates. Terms like "third party," "affiliate," and "business partner" were also deemed incomprehensible by the participants in the study. Based on the findings, it seems that people need better-crafted and -designed information in order for consent to be effective.

This article was written by Stephen M. Schuelle, Martha Neary, Elizabeth C. Adkins b, and Kristen O'Loughlin in 2018 [4]. Discusses the rise of mental health assistance applications for mobile devices No comprehensive investigation of the data security measures used by makers of health applications, particularly those aimed at mental health, has been conducted. It is critical that we assess the openness and integrity of these applications' data practices if individuals are going to rely on them for their mental health. The research examined the openness of data handling processes of mobile applications for depression that were retrieved from the Google Play and iTunes stores in October 2017. It also examined the privacy and security policies of these apps. They found 116 applications for mobile devices that met the criteria. Among these, 4% (5/16) were deemed acceptable in terms of transparency, 28% (32/116) were deemed doubtful, and 68% (79/116) were deemed unsatisfactory. A privacy policy was included in only 49% of the applications. Policies were far more common in programs distributed via the iTunes shop than in those distributed through the Google Play store. A privacy policy was included in 79% of the applications that collected identifiable information and 34% of the apps that collected non-identified information. When it came to data security, most of the applications we looked at were lacking in transparency. Apps offer enormous promise for expanding access to mental health services, whether as a supplement to therapy or for those who are hesitant or unable to seek out conventional in-person care.

Aiming to determine the current state of data privacy in critical digital assets held by Indian organisations, the Report (2018) set out to do just that. The study's primary objectives were Which third parties does the app/website share user data with, and how much of that data crosses international borders? How secure is the app/website's data handling? How open is the organization's privacy policy with regard to user data? Given the sensitivity of the topic, the research focused on Android apps aimed for children. Somewhat concerning were the results. It was found that 71% of children's apps had access to storage, phone details, and location. The App could not have operated without almost half of the permissions that were accessed. The vast majority of apps either didn't ask for permission or failed to verify the user's age when asking for it. The bulk of the apps included in-app advertisements and allowed users to buy things inside the app. Compared to their global counterparts, Indian Android apps request 45 percent more permissions up front. The disparity was most apparent in areas where Indian apps required 60-80% higher permissions, such as travel booking, shopping, and mobile wallets. A disproportionately large percentage of Indian apps have access to the following permissions: SMS, microphone, phone, and contacts.

Spyros E. Polykalas (2018) [6] noticed that Numerous personal and non-personal gadgets, including smartphones, tablets, laptops, sensors for IoT applications, and so on, produce vast amounts of data every day. Primarily, the goal of storing and analysing the information will be used to improve the services that are provided. When information can be traced back to a specific person, either directly or indirectly, we call it personal data. Many concerns about personal data privacy arise from data collecting, storage, and processing, especially when consumers aren't informed about how their data is being used. With over 3 million mobile applications, including social media apps, Google Play is one of the most popular personal applications stores. He wanted to see if their current procedures were in line according to the GDPR. Research revealed that Google Play's existing practices do not adhere entirely to the forthcoming framework. When it comes to matters such as safeguarding children from unauthorised app installations, users' lack of knowledge about the breadth of personal data processing, and the inability to install apps without granting complete access to personal data. A number of people think that app stores and developers should make certain changes so that the applicable processes are according to the standards set by the upcoming EU.

As a meta-study, The Report (2017) examines data protection and privacy in mobile applications by identifying relevant best-practices, open concerns, and gaps in the field and by analysing the aspects of the app development environment that affect these aspects. The paper examines several representations of mobile app ecosystems and provides an overview of the app development life cycle. In order to make developers more at ease with the legal obligations, we provide privacy and methods for safeguarding data during its inception and implementation.

Privacy in digital world

India has begun its historic transformation into a data

economy in recent years. More and more people in India are using digital services, which means they are creating massive amounts of data every day India is a rapidly developing nation data-generating countries, producing over 150 Exabytes of data every year.

Information is all around us and is created by almost every action we do. When data is shared, it creates efficiency, which is important in and of itself. There is the data that we knowingly provide, and then there is the data that is created automatically whenever we do anything, like when we book a flight, place an online food order, or utilise public transit. Several firms are prepared to pay a premium to have access to this Data, which proves its great value. With the advent of the internet and its near-universal availability, data has really become the new money. The fact that the data's full potential remains unknown is even more fascinating. The value of the data is being enhanced by the emergence of new applications as technology advances. Just as Facebook, the most popular media owner in the world, doesn't produce any content, Alibaba, the most valued retailer in the world, doesn't have any inventory, and Airbnb, the biggest lodging provider in the world, doesn't own any real estate, the world's largest taxi firm, Uber, doesn't own any cars. Nowadays, even a seemingly innocuous activity like calling a cab requires the user to enter their financial details, real-time location, travel history, and other personal information into a smartphone app. The way people do business, communicate, and make choices is being profoundly affected by data. Companies are increasingly amassing massive datasets on customer tastes and habits. There has never been an easier time to compress, store, alter, find, and evaluate data, making it easier to turn data into knowledge. The simplicity of data collection and the cheap cost of keeping and processing information have led to the widespread adoption of long-term data storage and the collecting of ever-increasingly-minor facts about a person, enabling the creation of comprehensive user profiles. Saving time during the checkout process is one advantage of using this data to build personalised user profiles based on customers' previous online activity.

Rather than Big Data, the problem stemming from this expansion is data pertaining to behaviours. Digital records provide more specifics on our purchases, thoughts, activities, and social interactions. More and more, this data is being utilised to deduce previously concealed aspects of our personalities. Our thorough online portraits, which are utilised for targeted marketing, suggestions, and customisation, are developed using it. Unexpected data smashups and data that isn't usually disclosed intentionally form the basis of such depictions. Even more concerning is the fact that these depictions may conflict with our public identities and self-perceptions.

Concerns such as who owns the data, who can access it, and how far can it be used raise serious concerns. The legal system is playing catch-up in every area of technology. The fact that several countries are requesting and requesting access to data from their citizens and corporations further complicates matters. Problems include data emending for access to essential services, travel, or even government benefits, the question of where privacy ends and national security begin to take precedence, and so on. By virtue of Article 21, As a fundamental right, the right to privacy is acknowledged in India. "The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution," in the case of K. S. Puttuswamy v. Union of India, the court determined.

Privacy as a human right

There is no country that does not have human rights. Just because someone is human doesn't mean they don't have the right to certain legal protections. Human rights have been formalised in a corpus of treaties and conventions. It is the purpose of international human rights instruments to protect human rights. Various international documents, including treaties, may categorised as Declarations and Conventions, make up these international instruments. Since its approval by the UN General Assembly in 1948, the Universal Declaration of Human Rights (henceforth "UDHR") lacks any power to be legally enforced. However, the UDHR is jus cogens since it is a human rights bible. International law, however, makes conventions legally enforceable. The "International Bill of Rights," the most significant the United Nations drafted the human rights framework, which outlines several rights. A list of basic human rights is provided by the UDHR, the ICCPR, and the ICESCR. Although the human rights guaranteed by these treaties are reinforced by a number of other international accords, it is unusual for any of them to make direct reference to safeguarding human rights via technological means (Australian Human Rights Commission 2018). There are domestic and regional organisations and institutions that work in tandem within the framework of human rights legislation on a global scale to offer robust remedial frameworks; furthermore, there is clear guidance on how to adapt human rights law to new contexts, such as those brought about by technological advancements.

Treaties ratified on a global scale acknowledge that everyone has the right to personal privacy. As a result, privacy is universally recognized as an essential component of human rights. Privatity and the freedom to refuse, honour and reputation, family, home, and communication is safeguarded against arbitrary interference by both treaties, such as the International Covenant on Civil and Political Rights (Article 17) and the Universal Declaration of Human Rights (1948).

Privacy and social media

With the rise of IT in the 1960s and 1970s, people started to worry more about their own space.15 In the '90s, social media took off and beyond-also known as social networking sites-was a game-changer because it made instantaneous online communication possible.

The realms of online communication and social media are quickly merging with privacy concerns. New kinds of socialising, sharing, and communicating have been made possible by the meteoric growth in popularity and extensive usage of social media and SNS. The privacy concerns brought up by this new mode of communication are novel.

A wide variety of websites that allow for two-way communication are collectively known as "social media" communication via the dissemination of news and other content via sites like Facebook, WhatsApp, Twitter, Orkut, MySpace, Instagram, and many more. The freedom of

expression and privacy are greatly affected by social media. Online Communities By tracking users' financial activities, companies like Google, Facebook, and many more are invading consumers' privacy. Corporate social media economic surveillance includes tracking prosumers, who are constantly engaging in UGC creation and sharing, profile and data browsing, social media interaction, community building, and co-creation. Personal information and online actions are constantly tracked and recorded by business websites' proprietors and the marketing agencies that work with them. They keep track of information, combine it, and analyse it. Because of this, they are able to learn a great deal about the interests and online habits of their customers and build comprehensive profiles for them. Platforms that rely on targeted advertising to generate revenue treat prosumers like a commodity. Economic user monitoring is made possible by the trade of funds for data access from users.

Inability to access the self

Another school of thought holds that privacy is better defined as "limited access" to one's own identity. The need to hide one's identity and blend in with one's surroundings is the foundation of this idea. Therefore, it is both similar to and maybe a more refined form of "the right to be let alone." Having little access to one's own thoughts and feelings might be confused with being alone at times. Being alone, cutting off contact with other people, is what we mean when we talk of solitude. The concepts of restricted access and right-to-be-left-alone both include the idea of solitude, but both theories go far beyond the concept of solitude to include freedom from governmental meddling, press incursions, and other forms of invasion. Privacy is more than just being alone, according to limited access ideas.

"Nothing is better worthy of legal protection than private life," E. L. Godkin said in the late 19th century, advancing an early version of the limited access theory. He meant that people should be able to keep their affairs to themselves and decide for themselves how much of their lives should be open to public scrutiny.28 Privacy was defined by Godkin as the "right to decide how much knowledge of his personal thought and feeling, and how much knowledge, therefore, of his tastes and habits, of his own private doings and affairs, and those of his family living under his own roof, the public at large shall have" (July 1890, same year as Warren and Brandeis's article).

Several modern thinkers have put forward limited-access ideas. Bok defines privacy as "the condition of being protected from unwanted access by others either physical access, personal information, or attention."30 "The condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited," says Hyman Gross when asked to define privacy. “Privacyisthe exclusive access of a person (or other legal entity) to a realm of his own,” argues Ernest Van Den Haag. An individual is entitled to privacy if he or she does not want other people to (a)observe, (b)use, or (c)invade, or otherwise impact, his or her private area. "A degree of inaccessibility is an important necessary condition for the apt application of privacy," says Anita Allen, another legal thinker. 33 David O'Brien, a legal researcher, contends that theorists that see privacy through the lens of restricted access formulations have substantial differences. Some people see restricted access as a personal decision, a way to manage who can see one's private information. For some, having restricted access is just the way life is. Privacy, according to O'Brien, "may be understood as fundamentally denoting an existential condition of limited access to an individual's life experiences and engagements," with an emphasis on the latter perspective. Given that not everyone gets to choose their level of confidentiality, it's crucial to remember that the two concepts are distinct. A certain amount of privacy is unintentional, mandatory, or even forced.34 Being alone is the essence of privacy, according to O'Brien. However, the idea of the individual's agency in deciding what parts of herself to expose to others is completely absent from O'Brien's conceptualisation. For instance, it is likely more accurate to interpret O'Brien's remark that an individual abandoned on an isolated island enjoys total alone as a condition of seclusion. A person's claim to privacy would be meaningless in a society devoid of other people since privacy is relational.

Conclusion

Privacy policies are difficult to understand and contain ambiguous language that leaves out relevant information or contain words that leave statements made in the privacy policy open to interpretation.2 Furthermore, privacy policies tend to be long boring documents with ambiguous and misleading language. Multiple studies in privacy policy readability found that although privacy policies are the only means for an organization to communicate data sharing and collection policies, the ambiguous, vague, and confusing language used undermines the effectiveness and purpose of the privacy policy.

More than 120 nations have already enacted some type of international privacy rules for data protection, ensuring that individuals and their data are provided with more stringent safeguards and restrictions. It is evident that international privacy rules for data protection will continue to change and improve to assure the protection of personal data across all use cases and scenarios, even some that have not yet occurred.

In general, the worldwide privacy rules for data protection adhere to or are influenced by the following five global privacy principles:

1. Notification entails notifying users, visitors, readers, and users of the policies in place to protect their personal data.
2. Choice and consent entails providing people with alternatives and permission about the acquisition, use, storage, and management of their personal data.
3. Access and participation entails ensuring that the proper persons have access to the information and use it in compliance with the necessary security measures.
4. Integrity and security entails ensuring that the data are secure, and that unauthorized access is impossible.
5. Compliance enforcement entails ensuring that a service, website, solution, and platform adhere to a regulation that mandates compliance.

References

1. Kamleitner B, Mitchell V. Your data is my data: A framework for addressing interdependent privacy infringements. Journal of Public Policy & Marketing.

2019;38(4):433-450.
2. Matthan R. Privacy 3.0: Unlocking our data-driven future. HarperCollins; c2018.
3. Bailey R, Parsheera S, Rahman F, Sane R. Disclosures in privacy policies: Does “notice and consent” work? NIPFP Working Paper Series No. 246. National Institute of Public Finance and Policy; c2018.
4. O'Loughlin K, Neary M, Adkins EC, Schueller SM. Reviewing the data security and privacy policies of mobile apps for depression. Elsevier B.V.; c2018.
5. Arrka. The state of data privacy of mobile apps & websites from India. 2018.
6. Polykalas SE. Assessing General Data Protection Regulation for personal data privacy: Is the end of the "take it or leave it" approach for downloading apps? The Seventh International Conference on Social Media Technologies, Communication, and Informatics, Regulation. 2018.
7. European Union Agency for Network and Information Security (ENISA). Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR. 2017.
8. FTC Staff Report. Mobile privacy disclosures: Building trust through transparency. 2023.
9. Westin AF. Privacy and freedom. New York: Athenum; c2017.
10. Bansal VK. Right to life and personal liberty in India. New Delhi: Deep and Deep Publications; c2017.
11. Basu DD. Law of press in India. New Delhi: LexisNexis Butterworths; c2020.
12. Basu DD. Shorter constitution of India. New Delhi: Wadhwa Publications; c2022.
13. Chabbra GS. Advanced study in the constitutional history of India. Delhi: Prakash Brothers; c2023.