INTERNATIONAL DEVELOPMENT PLANNING REVIEW
ISSN:1474-6743 | E-ISSN:1478-3401

PRIVACY: THE GARB OF RIGHTS IN THE DIGITAL AEON - CHALLANGES AND PROSPECTIVE IN INDIA

Dr. Priyamvada Tiwari[1] Mr. Keshav J. Jha[2]

Abstract:

It is said that law is dynamic and it changes its recourse as per the need of the society. Rights are not absolute in rigid sense. Though it has become the paramount source for sustaining the human being and it is one of the most significant aspects of living a dignified life. The constitution of India provides numerous rights to the people of India to sustain a well and dignified life. The Hon'ble Supreme Court of India has time and again discharged its duty for upholding and securing the fundamental rights for the citizens for a dignified life.

In current digital era, right to privacy has become one of the paramount issues for the people, despite the interpretation done by the Supreme Court of India for securing and upholding them as one of the basic fundamental rights for the citizen of India, it's violations are not being protected.

This has become one of the controversial and some of the academicians; scholar argues that there is least possibility of securing the right to privacy. Hence, it is a misnomer.
The paper argues about the right to privacy- its challenges regarding the violations in digital era.
Keywords: Right to Privacy, Violations, digital era, data protection

Introduction:

The Merriam Webster dictionary defines "Privacy" as "freedom from unauthorized intrusion".[3]
The Cambridge dictionary defines "Privacy" is someone's right to keep their persona matters and relationship secret.[4]
Privacy means to hide something from the interference of someone. It is the capabilities of a person or group of persons to hide the information from others as well as schedule themselves.
As far as the technology or the internet gets develop, the issue and challenges raises with the application of such technology or internet.
The explosive growth of the Internet has not only given individuals access to ever-new and convenient technology experiences, but it has also brought up significant issues that demand serious attention from the general public. The breach of personal privacy is among the most emblematic issues.

[1] Associate Professor of Law, Prestige Institute of Management & Research, Indore (M.P), India
[2] Assistant Professor of Law, Prestige Institute of Management & Research, Indore (M.P), India
[3] https://www.merriam-webster.com/dictionary/privacy
[4] https://dictionary.cambridge.org/

The development of Internet and the cloud computing system the data leakage has become more prominent problems among the citizens. Hence, the fundamental rights of the people are being compromised.

A surveillance system at home, to a mobile phone in the hand, to a registered app account, they all can become media for personal privacy leakage. In the age of this digital era everything is connected with one and other be it the aadhar card, mobile phone number, facebook, whatsapp or other social media and these connections somehow because the data leakage or privacy breach.

Research Methodology:

This paper is a combination of both doctrinal as well as non-doctrinal research using primary and secondary source. The primary source has been collected through questionnaire. The secondary source has been taken from books, journals, research papers and court judgements will be used to support the claims made in this paper.

The gap of the research will try to find out the problems associated with the infringement of Privacy in the digital world.

Sampling Method:

The data has been collected from 100 people from the universe to know the causation for privacy through snowball sampling method.

Right to Privacy an International Scenario:

Right to Privacy is recognized under Declaration of Human Rights, the International Covenant of Civil Rights and Political Rights as well as many other International and regional treaties it is recognized as a rights for an individual. Privacy is one of the fundamental problem associated with the individual in the digital era. Basically, it undermines the human dignity and other key values such as freedom of speech, and freedom of an association or other fundamental rights. Privacy preserve the human dignity through several facets of human life.

- Privacy appertaining to Information such as Medical Information, Personal Information, communication.
- Bodily Privacy, which is concerned with the people's physical selves against invasive procedures such as drug testing and cavity searches;
- Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.[5]

On the international scenario Right to Privacy can be traced back to 1361 in England, wherein it was mandated the arrest of peeping toms and eavesdroppers through the Justices of the Peace Act.[6]

[5] Gilc.org. (2020). Privacy and Human Rights - Overview. [online] Available at: http://gilc.org/privacy/survey/intro.html [Accessed 21 December. 2023].

[6] Thombre, S.P. (2019). Comprehensive study of Development of right to privacy in India with special reference to constitutional provisions. International Journal of Law, [online] 5(6), pp.117–122. Available at: http://www.lawjournals.org/archives/2019/vol5/issue6/5-6-43 [Accessed 19 Dec. 2023].

In international arena, many countries have formulated principles for the protection of Privacy. In 1776, the Swedish Parliament enacted the "Access to Public Records Act"[7] mandated the use of all information held by the government for justifiable purposes. It was stated in the 1792 Declaration of the Rights of Man and the Citizen that private property is sacrosanct and untouchable. In 1858, France established harsh penalties and outlawed the publication of personal information.[8]

The Universal Declaration on Human Rights has set a benchmark for protecting territorial and communications privacy stating therein under Art. 12 of the said declaration –

"*No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks"*[9].

Additionally, the European Convention on the Human Rights came into effect on 3rd Sept 1953. While respecting one's private and family life, it allowed public authority's interference only under exceptional circumstances.

Accordingly, the Convention stated that the Right to Privacy is not an absolute right and the Government can intervene private affairs of an Individual for the purposes of public safety and security.

The International Covenant on Civil and Political Rights (ICCPR) 1966, Article 17 of the convention states that -

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honour or reputation and everyone has the right to the protection of the law against such interference or attacks."[10]

Furthermore, the right cannot be taken away by jeopardizing the health, morals, rights, and freedoms of others.

Article 16 of the UN Convention on the Protection of Children (UNCPC), Article 14 of the UN Convention on Migrant Workers (UNCMW), Article 11 of the American Convention on Human Rights; all these have set out the right to privacy in terms similar to the UDHR.

Surprisingly, India is the signatory of all these conventions, however, no specific legislation has been formulated to secure such right to Privacy.

Constitutional and Judicial Perspective of Right to Privacy in India:

[7] Chydenius & apos; Legacy Today, A. (n.d.). The World's First Freedom of Information Act. [online] Available at: https://www.access-info.org/wp-content/uploads/worlds_first_foia.pdf [Accessed 23 December. 2023].

[8] The Rachel affaire. Judgment of June 16, 1858, Trib. pr. inst. de la Seine, 1858 D.P. III 62. See Jeanne M. Hauch, Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris, 68 Tul. L. Rev. 1219 (May 1994).

[9] Hrweb.org. (2020). UN Universal Declaration of Human Rights. [online] Available at: http://www.hrweb.org/legal/udhr.html [Last Accessed on 23 December 2023]

[10] https://law.dypvp.edu.in/blogs/international-perspective-of-right-to-privacy#:~:text=The%20International%20Covenant%20on%20Civil,the%20protection%20of%20the%20law [Accessed on 23 December 2023]

The privacy concern is not new; it is the matter of discussion from the very inception of the judicial system.

According to Justice Krishna Iyer, "Personal liberty makes for the worth of human person"[11]. Therefore, the notion of dignity and liberty are not independent of privacy. The draftsmen of the Indian Constitution were quite aware of the difficulties about the individual and they placed the right to life in the constitution as an essential right. The individual has the right to privacy from birth itself which is enshrined under Article 21[12] of the Constitution of India.

The Hon'ble Supreme Court of India has interpreted the constitution and given various dimensions to the Art. 21 in the light of its preamble. The preamble of the constitution is called the ideology of the constitution, therefore, to understand the intent of the constitution makers, the hon'ble court always refers to the preamble. The preamble has given the eminence to and guarantees the citizens of liberty of thought, faith and worship. Even the Hon'ble Supreme Court has not deterred in interpreting Art. 21, finding the scope for inserting all the rights under the article which is not expressly mentioned in the Constitution.

The right to privacy came into picture from the case of ***Kharak Singh Vs. State of U.P***[13] wherein the accused was put under surveillance and he was chased by the Police at night. It was contended that the term 'personal liberty' is used in Art. 21 as a compendious term to include within itself all the varieties of rights which go to make up the 'personal liberties' of man other than those dealt within the clauses of Art. 19 (I). While Art. 19 (1) deals with particular species or attributes 'of that freedom, 'personal liberty'. It was also contended by Subba Rao and Shah, JJ. that the Right to privacy is fundamental right under Article 21 and 19 (1) (d) of the Constitution of India. The U.P police regulation providing for continuous surveillance and under consideration were struck down.

In the year 1975, there were revolution for the Right to Privacy in India. In case of ***Gobind v. State of MP & Anr.***[14], the Supreme Court introduced the compelling state interest test based on American jurisprudence. The court ruled that an individual's right to privacy would have to yield to a more expansive governmental interest, the substance of which must be compelling. Over time, the privacy sphere has broadened to encompass sensitive personal data, including biometrics and medical records.

In 1977, the Supreme Court categorically ruled in the telephone tapping cases of ***PUCL v. Union of India***[15] that people had a right to privacy over the information they communicated over the phone. Thus, it can be seen from a number of decisions that while the right to privacy was acknowledged, its exceptions were also given appropriate consideration.

[11] https://www.intolegalworld.com/article?title=right-to-privacy, visited on 15/12/2023 at 10:03 PM
[12] "No person shall be deprived of his life or personal liberty except according to a procedure established by law."
[13] 1963 AIR 1295, 1964 SCR (1) 332
[14] 1975 SCC(2) 148
[15] AIR 1997 SC 568 / (1997) 1 SSC

The question for Privacy has been centered public discourse through the concept of ADHAR, the government scheme, wherein the individuals are allotted a unique ID after registering it through giving their biometrics such as fingerprints and iris scan and demographic details.

The scheme was challenged in the apex court through the case titled as ***Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.***[16] In this case, the nine-judge bench unanimously upheld the right to privacy as a basic freedom guaranteed by the Indian Constitution. The Court decided that the right to privacy was a basic component of liberty, autonomy, and dignity and that it was essential to the freedoms protected by all fundamental rights.

The Hon'ble Court also contended that "The right to privacy is inextricably bound up with all exercises of human liberty – both as it is specifically enumerated across Part III, and as it is guaranteed in the residue under Article 21. It is distributed across the various articles in Part III and, mutatis mutandis, takes the form of whichever of their enjoyment its violation curtails".

Right to Privacy in the age of Internet and Social Media:

Everyone in India has the right to free speech and indeed it is the democracy which has given this right. The media's responsibility in the modern day is to provide the public with all the accurate information at its disposal. The media need to provide information that inspires ideas and aids in decision-making. People are granted freedom by the media to choose what news they want to hear, but this freedom shouldn't be unrestricted. Individuals ought not to abuse this liberty. Should they abuse this freedom in any way, they ought to be held responsible? There isn't a specific common law enactment that offers protection with regard to web-based social networking. The principles of general security also apply to the realm of social media.

Nonetheless, the most of the discussion and references made in this area are about online social networking; however, we will specifically use Facebook as an example and make references to it in this way.

The main focus of the problem with internet networking is "assent" and "open area." The Data Protection and IT Act's statutory law of security, as it is properly stated, derives from the tort law of confidence, which is why it is a "assent reason" show. As previously mentioned in the previous sections, it follows that approval of a demonstration that generally may have constituted a breach of security section would dissect the applicability of each and every element of both complex and statutory protection law.

Having said that, Facebook has recently been plagued by security lapses that include data sharing with websites. This created a problem since, whenever a customer visited a website, his profile would show the address they used in other friends' news feeds.[17]

Stalking attacks are extremely common on social media networks. Using an online mob of anonymous, self-organized groups to target specific people and incite defamation, threats of violence, and technological attacks is one of the main strategies used in stalking. Social networking is utilized to foster trust between the victim and the offender. A perpetrator is someone who may

[16] (2017) 10 SCC 1, AIR 2017 SC 4161

[17] This was implemented by using "Beacon" developed by Facebook for this purpose. See http://www.facebook.com/press/releases.php?p=9166; See e.g. http://www.washingtonpost.com/wp-dyn/content/article/2007/12/12/AR2007121200041.html

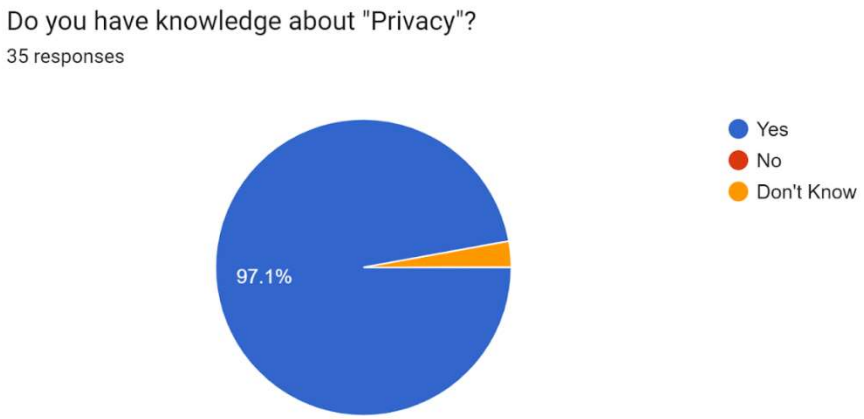
commit an immoral, unlawful, or destructive act. Confidential information sent by the victim, such as images and videos, might be intercepted, stolen, and misused by the perpetrator for extortion. Social media companies are also accountable for identifying users who have such nefarious intents, blocking them, and launching the proper legal proceedings in accordance with the law.

Challenges to Right to Privacy and its Prospective in Digital Era:

India has demonstrated significant progress in data protection with its efforts to outlaw Chinese technologies and support domestic digital solutions with the "Made in India" campaign. Additionally, the nation has developed laws pertaining to cyber security and taken action to stop cybercrimes. But there are still problems, such the fact that cyber security incidents frequently go unresolved and that there isn't a convenient way to deal with them. The prevalence of online frauds leaves people open to privacy violations and data breaches.

India has also passed laws and implemented policies to combat cybercrime and improve online privacy. The principal law covering cybercrimes and digital transactions in India is the Information Technology Act, 2000 (IT Act). In 2008, it was modified to offer an extensive.

To protect cyberspace and stop cyberattacks, the Indian government unveiled the National Cyber Security Policy (NCSP) in 2011. The NCSP's main objectives are to strengthen security protocols, develop a collaborative and information-sharing environment, and advance cybersecurity awareness and education. It also highlights the creation of industry-specific Computer Emergency Response Teams (CERTs) and the enhancement of incident response capabilities.

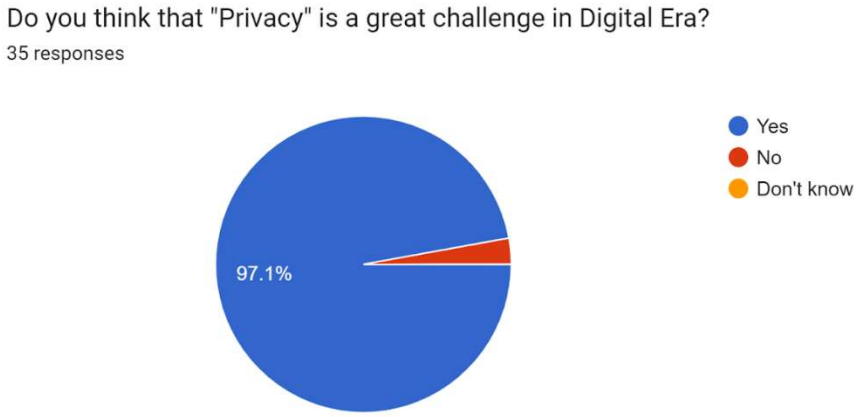


Today's world is paranoid. We can never be positive of the manner in which we are being watched, thus we are always suspicious that we are being followed. In this way, technology is unpredictable and invisible. The fast technological advancement that humanity is currently experiencing is associated with a number of serious concerns. The dread of total privacy loss is one among them. One sign that this scenario might come to pass is the dubious privacy practices on the internet.

"Internet users have only recently begun to realize that every single thing they do online leaves a digital trace," according to reputable magazines."[18] The most unsettling aspect appears to be the idea that individuals are being watched without their knowledge.

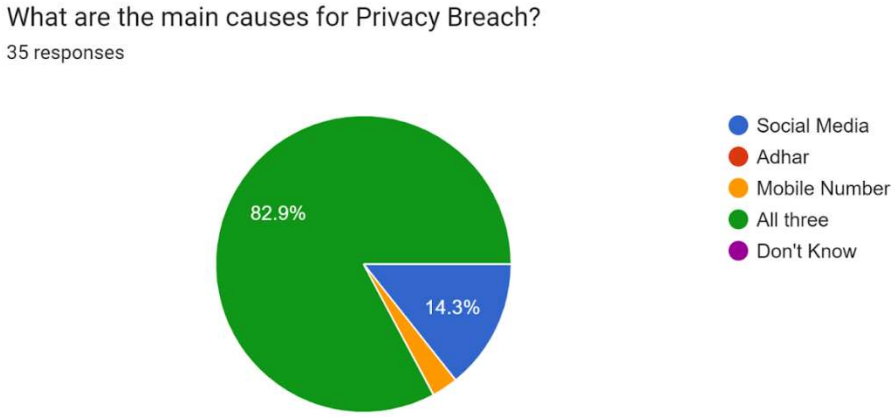
The most frequent risks associated with data collection systems are prejudice and disclosure. While providing their respective services, businesses such as banks, hospitals, and retail supply chains gather a lot of personally identifiable information. In order to obtain profound understanding, make wiser judgements, and provide value-added services, this data will be analysed.

There are numerous of challenges wherein it becomes impossible to protect the data from being breached. Some are being listed herein: -



A. Lack of awareness

Toady everything is linked with a single mobile phone number and due to unawareness, people share the details to unauthorized users and the same causes harm to their personal information.



B. Social Media Platform

[18] The Economist, Horror Worlds, http://www.economist.com/node/17388328 , last visited 23 December 2023.

Social Media platform has immense challenges for protecting privacy. In today's world everyone is connected through the social media and there is no such regulation for maintaining the privacy of an individual.

Suppose if any individual searches for something on the Google platforms, suddenly, he gets notification of all the searches on other social media platforms, that actually reflects the breach of privacy. Ultimately, no regulations exist for curbing those situations and such breach of privacy.

C. Adhar card

Although, the decision came in the case titled as ***Justice K.S Puttaswamy Vs. Union of India***[19] that the Adhar is not mandatory except in government schemes as every information is linked with the adhar of an individual. Despite there are several occasions wherein the adhar is being demanded and there is no such proper forum to complain for such acts.

Everyone has the adhar card, therefore it has become necessary to have adequate cyber security measures to protect and maintain the privacy of individuals.

D. Mobile Number

In the modern age of digital era, the circulation of mobile number is not safe as everything is connected with a single mobile number, therefore breach of privacy occurs and cannot be denied.

Apart from the above mentioned factors, there are numerous factors existing for the breach of Privacy. Individual privacy has become the fundamental necessity for an individual to be secured and protected. The advancement of technology can raise many more challenges for the Privacy in the future such as:-

The breach of privacy may enhance cybercrime. Therefore, it is needed to secure the privacy of an individual.

In 2018, 208,456 cyber-related offences were reported. More cybercrimes were reported in the first two months of 2022 than there were in the whole of 2018.

[19] (2017) 10 SCC 1

Throughout the epidemic, the numbers increased even more dramatically, with reported crime rising from 394,499 cases in 2019 to 1,158,208 cases in 2020 and 1,402,809 crimes in 2021. India had a 15.3% rise in cybercrime between Q1 and Q2 of 2022.
In addition, the number of Indian websites that have been hacked in recent years has been rising. 18,560 or so websites were compromised in 2018. A total of 26,121 sites experienced hacking in 2020. In 2021, ransomware attacks affected 78% of Indian companies, and in 80% of those cases, data encryption was the outcome. By contrast, the mean proportion of attacks was 66% with the average of 65 %. [20]

Prospective Solutions for Privacy Breach:
The right to monitor and control one's personal information posted on digital networks is referred to as privacy. It includes preserving the privacy, accuracy, and usability of data. Safeguarding the privacy of your data is essential to avoiding unwanted access, improper use, or commercialization of your private data.

Principles of Privacy and Protection:

The methods and procedures used to prevent unauthorized access, loss, or theft of personal data are collectively referred to as data protection. Safeguarding confidential information with appropriate data protection reduces the likelihood of identity theft, data breaches, and cybercrime. The principles of privacy and data protection are based on:

- **Consent and Transparency:** Get people's express, informed consent before collecting their data. Transparently state the goals and methods of data collection.
- **Purpose Limitation:** Only gather and use data for clearly defined, authorized reasons that are communicated to the individuals.
- **Data Minimization:** Put strong security measures in place to guard against loss, alteration, and unauthorized access to data.
- **User Rights:** Respect people's rights, including the ability to see, update, and remove their personal information.
- **Accountability:** Assume responsibility for data processing operations and abide by all relevant data protection laws and rules.
- **Organizational Data Protection Practices:** A documented policy outlining the safeguards for sensitive data must be in place. Topics like data retention periods, encryption, and access control should all be covered in the policy. It should also include explicit instructions on how to report breaches and what to do in the event that one happens.
- **Strong and Unique Passwords:** For each of your online accounts, create a unique, strong password, and don't use the same one twice. To safely keep and handle your credentials, think about utilizing a password manager.

[20] https://aag-it.com/the-latest-cyber-crime-statistics/ (Last visited on 27 December 2023, 7.35 PM)

- **Two-Factor Authentication (2FA):** In order to further secure your accounts, turn on 2FA wherever you can.
- **Regular Software Updates:** To guarantee that your operating system, programs, and antivirus program have the most recent security patches, keep them updated.
- **Phishing Awareness:** Be wary of dubious calls, emails, or messages requesting personal information. Steer clear of dubious connections, and make sure a website is legitimate before entering any information.
- **Social Media Privacy Settings:** Examine and modify your privacy settings on social media to manage the visibility of your personal data.
- **Unauthorized access or permission:** while using any application don't give the access or permission for allowing the personal data or information circulation without having proper knowledge. One of the major causes is to give unauthorized access in the application and accepting the cookies.

In order to avoid unintentional or deliberate violations of organizational data protection regulations, it is imperative that staff receive training on best practices for data privacy. Regular training sessions emphasizing the value of securely handling data, recognizing phishing attacks, and understanding how to report suspicious actions should be provided to staff members. They should also be taught the importance of password management and the risks associated with disclosing private information to unauthorized parties. Establishing strong data protection procedures and routinely training staff members on data privacy best practices should be top priorities for organizations. By doing this, you can both assist reduce the risk exposure from potential cyber threats and create an environment where all departments within the company take shared responsibility for safeguarding personal information.

Concluding Observations:

In this digital era, it seems that the privacy has become one of the challenges for the individual. Basically, the privacy breach occurs due to the internet connection infects the individual's system, sometimes some applications didn't work until given access to the GPS. The main causation for privacy breach are: third-party data sharing, and cyber threats, inadequate cybersecurity measures and evolving technology, etc. Apart from this Privacy breaches occur due to various factors: inadequate cybersecurity measures, human error, malicious intent, outdated software, weak passwords, insufficient encryption, third-party vulnerabilities, and the rapid expansion of data collection without corresponding protective measures. therefore, it is high time to make the proper regulation to curb this situation. As the Hon'ble Supreme Court in the case titled as ***Vinod Kaushik & Anr. V. Madhvika Joshi and Ors***[21]., held that accessing email IDs of other individuals unauthorizedly is a criminal offence under Section 43 of the Information Technology Act and calls for stringent action.

The government should come into forefront for fighting this situation. The research shows that the main causation for privacy breach is social media, mobile number, adhar etc. therefore, it is needed

[21] WP(C) 160/2012

to make stringent laws pertaining to these malicious things. The right to privacy is the fundamental rights of the citizens.