National Journal of Advanced Research
ISSN: 2455-216X; Impact Factor: RJIF 5.12
Received: 03-07-2019; Accepted: 06-08-2019
www.allnationaljournal.com
Volume 5; Issue 4; October 2019; Page No. 43-46

Privacy and data protection in cyberspace

Nikhil Sanadhaya[1], Ayush Kumar[2]
[1-2] Seedling School of Law and Governance, Jaipur National University Jaipur, Rajasthan, India

Abstract
With the advancement in technology and emergence of internet and then various social interaction platforms such as facebook, instagram, snapchat, etc. the issue of privacy was initial not taken into concern but now it has become a major issue. In recent times there was news that European Union has fined Google with billions of dollars for the privacy breach. Last year a controversy related to Cambridge analytica and popular social media platform facebook grabed huge attention and facebook received huge criticism after this controversy. In cyberspace the issue related to privacy and data protection has became a major concern for legal intellectuals all over the globe. Globalization has given acceptance of technology in the whole world, as per growing requirement different countries has introduced different legal framework like DPA (Data Protection Act)1998 UK, ECPA(Electronic Communications Privacy Act of 1986)USA etc. from time to time, but in India there is no such comprehensive legal framework that deals with privacy issue. To handle major cyber challenges we refer ITA Act 2008 that was built with the motivation to facilitate e-commerce and hence the privacy was not prior concern in IT act. This suggestive framework provides comprehensive solution as per present and future requirements of privacy. As rightly said "true power of any law lies on its ability and ease of enforcement".

Keywords: privacy, data security, data protection, social media

1. Introduction
Privacy may be defined as a right of an individual's to determine when, how, and to what extent she will release personal information. A reasonable expectation of privacy demands that an individuals may proceed on the assumption that the state may only violate this rights by recording private communication on clandestine basis when it has established to the satisfaction of detached judicial officers that an offence has being committed and that interception of private communication stand to afford evidence of the office [1]. In this case the constitutional validity of Aadhar was challenged and it was held by the honourable Supreme Court where the validity of Aadhar was upheld but the court restricted state's action to intrude one's privacy by recognising privacy as a fundamental right. After this judgment it is the duty of the legislation to enact certain laws safeguarding individual's privacy both in real and virtual world. There are several legislations in developed countries like USA, Switzerland, European union and other actions such as providing guidelines, framing of Policies, etc.

We know that India is an emerging economy and several multinational companies are establishing their offices in India such as Google, Microsoft, Facebook, etc. The companies like Facebook, Google adopts the business model collecting the data for the purpose of which the revenue is generated but in recent year these companies started selling their customers private data to advertising companies to even some anonymous companies which harness this data for immoral and illegal use. for example the controversy in the year 2018 that the company called Cambridge Analytica had use the information of users of Facebook and used in for the Presidential Election Campaign in USA. There are several instances where Facebook and Google have been fine with huge amount for the breaching privacy of the Citizens of European Union. This shows that privacy and data protection have became a crucial concern for the nations. Hence in order to achieve this aim it is necessary to frame strong legislation. They are functioning here without any legal framework in the sense of protecting the privacy of individuals of India. There are some provisions (such as sec. 43 and sec. 63, etc) under IT (Information Technology) act, 2000 but they are not adequate for protecting the privacy of individuals. Right to privacy is under severe threat in the cyber space in India.

Objective
To focus on privacy and data protection in Cyber Space with respect to India in comparison to other countries. This paper primarily puts emphasis on the action taken by the countries in order to protect their privacy and data of the citizens and eventually giving rise to laws regarding privacy. Privacy against illegal intervention.

Concept of Privacy and Data Protection in Today's Modern World
"John, you're a Timex watch in a digital age", snidely quips Thomas Gabriel, the brilliant, but maniacal, cyber-villain of *Live Free or Die Hard,* the fourth (and some would argue best) entry in the *Die Hard* film series. The modern world is ruled by data. Data is the lifeline that not only fuels our decision-making but also supports the experiences which we have and caters to our day-to-day lives. And the Internet becomes the big kahuna of data. Market surveys competitor analysis and even everyday decisions of a normal human being are driven by the

Information and data received via social media channels search engines, blogs etc. Gone are the days when we used to dust out and pore over old files in a dark corner of a library to read age-old information on an age-old topic. Today, one has all the information that one needs on one's fingertips, quite literally. Just whip out your smartphone and connect to the internet.

Have you ever filed taxes or made a phone call? Do you own a smartphone? Have you ever used the internet? Do you have a social media account or wear a fitness tracker?If you answered yes to any of these questions, you have been sharing your personal information, either online or off, with private or public entities — including some that you may never have heard of.

Sharing data may bring benefits, and it has often also become necessary for us to do everyday tasks and engage with other people in today's society. But it is not without risks. Your personal data reveals a lot about you, your thoughts, and your life. These data can easily be exploited to harm you, and that's especially dangerous for vulnerable individuals and communities, such as journalists, activists, human rights defenders, and members of oppressed and marginalized groups.

With so much exposure to the Internet and, consequently, the exchange of terabytes of data, a common problem that has risen is the security of the exchange. Recently, the world has been plagued by ransom wares and malwares which have brought multinational giants on their knees, for days. Therefore, security is a legitimate concern. What does an individual or a SME or a start-up do when giants falter?

In spite of the fact that privacy only became a generally accepted right in the 19th-20th century, privacy had existed long before this era. Privacy has a very long history; it has its origins already in the ancient societies. Even the Bible has some passages where the violation of privacy appeared in its early form, where shame and anger followed the intrusion into someone's private sphere. It is enough to think of Adam and Eve, who started to cover their bodies with leaves in order to preserve their privacy [2]. From a legal point of view, the Code of Hammurabi contained a paragraph against the intrusion into someone's home, or the Roman law also regulated the same question [3].The idea of privacy traditionally comes from the difference between "private" and "public" which distinction comes from the natural need – as old as mankind – of the individual to make a distinction between himself/herself and the outer world. Of course the limits between private and public differ according to the given era and society which will cause the on-going change throughout history of what people consider private [4].

Given the fundamental complexity of contemporary data processing relationships there is acute need for a systemic and structured normative approach to data protection of which personal data protection is a part. The claims of privacy and personal data protection need to be considered in the context of prevalent trends of freedom of information and expression, as well as, competing claims of 'security'. Developing national and international personal data protection regimes needs to acknowledge the need for broad and systemic safeguards to privacy online that go far beyond explicit personal data processing regimes.

It goes without saying that innovations in information technology will continue to make us more productive, help us solve difficult and challenging problems, entertain us, allow us to communicate with virtually anyone in the world instantaneously, and provide all kinds of additional, and previously unimaginable, benefits. For instance, who wouldn't want an app that tells you the optimal time to go to the restroom during the movie you're about to see at your local theater? These new technologies are not only compelling, but also intoxicating and addicting—leaving us with a huge blind spot that puts us at great risk of losing our property, our privacy, our security and, in some cases, our lives.

We have built an incredibly complex information technology infrastructure consisting of millions of billions of lines of code, hardware platforms with integrated circuits on computer chips, and millions of applications on every type of computing platform from smart watches to mainframes. And right in the middle of all that complexity, your information is being routinely processed, stored and transmitted through global networks of connected systems. From a security and privacy perspective, we are not only concerned about the confidentiality, integrity and availability of the data contained in the systems embedded deep in the nation's critical infrastructure, but also of our personal information.

The Indian Constitution in Article 19(1)(a) provides the right to freedom of speech and expression, which implies that a person is free to express his will about certain things. A person has the freedom of life and personal liberty, which can be taken only by procedure established by law under Article 21. These provisions improvably provide right to privacy to individuals and/or groups of persons. The privacy of a person is further secured from unreasonable arrests under Article 22 and under Article 25 the person is entitled to express his wishes regarding professing and propagating any religion. The privacy of property is also secured unless the law so authorizes i.e. a person cannot be deprived of his property unlawfully under Article 300-A. The personal liberty in Article 21 is of the widest amplitude and it covers a variety of rights which constitute the personal liberty, secrecy, autonomy, human dignity, human right, self-evaluation, limited and protected communication, limiting exposure of man and some of them have been raised to the status of fundamental right viz. life and personal liberty, right to move freely, freedom of speech and expression, individual and societal right and given protection under Article 19.

Case Studies on Privacy and Data Protection

Indian Cases

- On 11 Feb 2010, the Home Ministry could not get the Cabinet Committee on Security's (CCS) nod to set up its ambitious NATGRID -- National Intelligence Grid -- as questions over safeguards for individual's privacy are learnt to have forced it to hold the proposal for further discussion. Though the proposal will finally get CCS approval, it will happen only after the ministry comes out with detailed information about the inbuilt safety mechanism, according to government sources. The proposed NATGRID -- a world-class integrated national security database -- will facilitate quick access to information on an individual -- like details of his/her

Banking, insurance, immigration, income tax, telephone and Internet usage.

- Government of India has launched a massive project to issue unique identification numbers (UID Nos.) to all residents in the country – close to 1.2 billion – by capturing their personal particulars along with biometrics such as fingerprints, iris scan and facial image. This has thrown up several privacy challenges. Data will be captured by thousands of registrars and sub-registrars throughout the country, sent over networks for storage centrally. Central data will be accessed for de-duplication whenever a new entry of UID is to be created. This poses privacy challenges at all stages of collection, processing and storage.

In another landmark case the Supreme Court of India further developed the law of privacy by holding that domiciliary visit of the police and disclosure of the information [5]. These disclosure of the information approaching the modern data protection concern. In *R* Rajagopal vs. *State of* Tamil Nadu [6] the petitioner was the editor,printer and publisher of a Tamil weekly magazine published inMadras who sought an order restraining the State of Tamil Nadu from interfering with the authorized publication of theautobiography of Auto Shankar, a condemned prisoner awaitingthe death penalty which was based on public records. In this case the court reaffirmed that the right to privacy is implicit in the right to life and liberty guaranteed in Article 21 ofthe Constitution. The Court also affirmed that the 'right to be letalone' for every citizen of this country to safeguard their privacy. After all this in K.S Puttaswamy vs. Union of India [7] privacy was held as the fundamental right under Indian constitution. This judgment is expected to create a huge impact on Indian jurisprudence regarding privacy issues.

Foreign Cases

1. Three Google Executives on privacy violations were convicted by an Italian Judge in Milan court on 24 February 2010 because they were found guilty of failing to comply with Italian privacy code in allowing a disparaging video to be posted online. Prosecutors argued that Google broke Italian privacy law by not seeking the consent of all the parties involved before allowing it to go online. The video at the centre of the case was posted on Google Video in 2006 shortly before the firm acquired YouTube. But the video was removed as soon as it was brought to its attention and that the firm also provided information on who posted it. This decision was described by Google as an "astonishing" attack on freedom of expression on the Internet.
2. In November 2009, Facebook issued a proposed new privacy policy, and adopted it unaltered in December 2009. This new policy declared certain information, including "lists of friends", to be "publicly available", with no privacy settings; it was previously possible to keep access to this information restricted. Due to this change, the users who had set their "list of friends" as private were forced to make it public without even being informed, and the option to make it private again was removed. After Facebook's recent privacy settings
3. "Adjustment" in December 2009, the social network reported on 1 February 2010 that 35% users who had never before engaged with their privacy settings took the initiative to do so instead of accepting the updated suggestions put before them by the social network.

Privacy laws and data protection

[8] The concept of Data protection has some directive in different countries. The European Union has sophisticated Data Protection Law. Under EU law, personal data can only be gather legally under strict conditions, for a legitimate purpose. Furthermore, persons or organizations that collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners that guaranteed by EU law. While there are concerted efforts in the administration calling for privacy legislation covering various types of data the large number of bills in Congress dealing with privacy issues suggests that the U.S. may continue to take a piece-meal approach to privacy legislation.

In India, the main principles on privacy and data protection enumerated under the Information Technology (Amendment) Act, 2008 are defining data, civil and criminalliability in case of breach of data protection and violation of confidentiality and privacy.

The Information Technology Act which came into force in the year 2000 is the only Act to date which covers the key issues of data protection, albeit not every matter. In fact, the Information Technology (Amendment) Act, 2008 enacted by the Indian Parliament is the first legislation, which contains provisions on data protection. According to section 2(1)(o) of the Act, "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed or is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer". The IT Act doesn't provide for any definition of personal data and, the definition of "data" would be more relevant in the field of cyber-crime.

Conclusion

Despite the very long history of privacy, after several centuries it is still a very topical question. Legal scholars were very interested in defining privacy and the right to privacy, then international and regional legal human rights conventions also regulated the question. However, some problems concerning privacy protection still exist and there are still a lot to do: it isespecially the lack of the definition of privacy and the lack of horizontal effect which should be revised in the light of the innovations of the 21st century. As a result of my study I found that the possible solutions may be the following. First, a flexible interpretation of the notion of privacy is needed. Second, protection should be guaranteed against not only the state but also business entities and/or individuals. And third, technology itself must be taken into consideration, still staying technologically neutral at the level of the regulation, but enforcing principles like privacy impact assessment, and giving more importance to the education of the users.

References

1. RVs. Duarte, 1990, 1 SCR 30
2. Konvitz MR. Privacy and the Law: a Philosophical Prelude. Law and Contemporary Problems. 1966; 31:272.
3. Solove DJ. Nothing to Hide: the False Tradeoff between Privacy and Security. New Haven & London: Yale University Press, 2011, 4.
4. Solove DJ. Conceptualizing privacy. California Law Review. 2002; 90(4):1132-1140.
5. Govind vs. State of Madhya Pradesh, AIR 1975 SC 1378
6. (1994) 6 SCC 632
7. (2017) 10 SCC 1
8. Handbook of European Union Data Protection laws, Accessed September 2, 2019,http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protectionlaw-2nd-ed_en.pdf.)