

ADVERTISEMENT TARGETING: A SEEMING ATTACK ON DATA PRIVACY

-Harshit Adhikari & Falguni Mundhra¹

I. INTRODUCTION

“Privacy is not an option,

And it shouldn't be the price we pay just for getting on the internet.”

Our world is filled with all sorts of people. Some good and some bad. there are always those who wish to take advantage of us and benefit from it. Are we comfortable with sharing all our information with strangers? If not all of it then exactly how much are we willing to share? Are we really in control of the amount of information that is available to others?

Everyone has things that they wish to keep to themselves, be they physical or maybe even digital. The fear of the consequences of these things being exposed to unwanted entities is why everyone values privacy and security so much in the case of both, physical and digital matters.

We live in the digital era, the era of data. Data is the oil of the modern world.² We want our data to be used only for our benefit, we want it to enhance our digital experience but not for causes that will harm us. Some amount of our data being accessible to the government is a necessity for matters of national security. But there should be a limit to that and there should be measures to ensure that these limits are not exceeded. But there are always people who wish to exploit others for their own gain. We see regular evidence that there are possibilities of our data being exposed or misused by different entities. Hence the current worldwide rage about data privacy. Data privacy in a general sense refers to the ability of the user to control the extent to which their personal information is made available to or communicated to others. The data in question can be the user's identity, location, contact information, or information regarding behaviour on the internet.

¹ The authors are students in their II year at KIIT school of law, Odisha.

² Stephen J. Biglew, Data Privacy (Information Privacy), TechTarget, <https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy>

Advertisement Targeting: A Seeming Attack On Data Privacy

II. IMPORTANCE OF DATA PRIVACY IN THE MODERN AGE

Now more than ever before we need the ability to handle data. The modern world is pacing toward digitization. There is an overflow of data. With that, there is an increase in the need to be able to keep this data secure and private. We are striving our hardest to have all sorts of processes and documents available online this increase in usage of the web has increased the importance of data privacy. Companies behind applications, social media, and websites collect data about us to be able to provide services to us. The govt. and these private corporations that collect our data claim to be using it for good purposes like ensuring the security of our nation or things like better experiences in the digital world. But how can we be sure of that? Remember the last time you talked to a friend about something and an ad for it popped up on your browser? A few times and it could have been a coincidence but the sheer frequency is what scares people and makes them doubt the words of the big data companies.

We have seen many cases where someone's data is compromised and they are blackmailed to not have their data revealed to the general public. Sometimes these incidents include information like bank details which cause huge financial losses. These create doubts in people's minds and cause them to refrain from engaging online. People need assurance that their privacy is ensured to feel safe in online activities. Organizations need to show people the several steps they are taking to ensure data privacy so that people trust them with their data.³

There are various ways our data can be misused after a breach in its security or if people do not possess the ability to control the way their data is stored or used:

- There can be harassment or fraud faced by users through the hands of criminals

³ CLOUD FLARE, What is Data Privacy?, <https://www.cloudflare.com/learning/privacy/what-is-data-privacy/#:~:text=Data%20privacy%20is%20also%20important, trusted % 2 0 with % 20 their % 20 personal % 20data.>

- Entities can sell the private data of users to advertising agencies so that the user receives unnecessary marketing or advertisement
- The tracking of individual's activities can lead to limited expression of opinions and limited online activity, especially in places where the govt. is repressive.

The level of privacy that we are afforded right now is not desirable enough for a lot of people. Some companies still do not place adequate security measures around the data they collect from gullible users in the name of better services. The lack of said security may lead to a breach which can lead to compromise the privacy of the users.

Does it not become scary when the internet seems to know things about us that we did not share?

III. A SEEMING ATTACK ON DATA PRIVACY i.e. TARGETED ADS

Sometimes the type/amount of data being collected exceeds our expectations. How many times have you opened your social media and come across an advertisement for a product your friend told you about? Even though we never searched about it, we got ads about it. We get ads of things that we heard at some event. How does that happen? Are our devices listening to us? If not, then how do these advertising companies find out? Sometimes we get advertisements about things we just happened to think about, we get these ads without even talking about these things. Do these companies know so much about us that they can guess the kind of things we might like or the things that might be the subject of our conversations? Would that not require them to know our friends, their interests, and their backgrounds as well? Even the sources mentioned above would not allow companies to understand us so thoroughly. Do these companies really have access to so much information about us? The unfortunate answer to this question is YES.

Advertising companies realized that since random advertisements are everywhere, the general public has gotten pretty good at ignoring them. This has forced advertising agencies to take a few steps to generate and provide us with ads that we are most likely to engage with. These ads focus on our specific traits, interests, and our preferences. The advertisers discover these after tracking our activities on the internet.

Advertisement Targeting: A Seeming Attack On Data Privacy

Let's say we search for a CD of your favourite band on the internet, the website on which you look for it, uses it to store cookies on your device which tells the other websites, that you visit in the future about your preference which then use it to show you advertisements which are as similar as possible to the object you were looking for i.e. they may show you ads for T-shirts of the same band or CDs of some other similar band.

Aside from cookies, advertisement companies also learn about us in different ways like checking our search engine history and they even try to find our personal information from social media. These ads target us across different devices as well, these make it seem like nothing we do is private, these companies use all their means to find out about our age sex religious relationship status, etc. to give us ads that are as relevant to us as possible.

These advertisements that we get after our data is revealed to different entities, are called targeted advertisements. To make the practice of targeted advertisements seem more ethical the websites or services we use give us an option on whether we would like to store cookies or not, but is it really an option? We can disagree to store cookies but then we would be unable to use the necessary website application or any other facility. Simply said we are bound to accept these cookies.⁴ We need to be able to access all our necessary websites without being forced to give permission to unknown entities to access information about us. The fact that we are being forced to accept giving up our data by our own hands because of a subtle threat from these huge data companies should be alarming to us all. Those who find this alarming have been demanding government intervention in these areas for a long time. We need proper laws and mechanisms to feel safe on the world wide web because ensuring proper security and data management is the only way to get more people to interact online and go about their activities without feeling heavily restricted.

IV. LAWS RELATING TO DATA PRIVACY

There exist several legislations dealing with information technology, contracts, intellectual property, and criminal acts, that ensure our security, offer protection, and impose civil and criminal responsibility, but even today in this modern era where data is everything, India does not have a single, comprehensive law that protects privacy or personal data. Currently, India's

⁴ AMLEGALS, Targeted Advertisements- An Invasion Of Privacy?, accessed on 15.01.2023, <https://amlegals.com/targeted-advertisements-an-invasion-of-privacy/#>

legal foundation for data protection and privacy is provided by the rules laid under the Information Technology Act, 2000 ("IT Act"). The very thought of sensitive private data is discussed through these laws.

In addition to suggesting that privacy laws be established, the Justice Shah Report on Privacy in 2012 identified 57 particular sectoral and policy recommendations that already exist that have ramifications for privacy and must therefore be changed as soon as the new legislation is passed.⁵ While the personal data protection bill is pending in the parliament, there are other acts and provisions that govern the data privacy matters, such as,

1. Constitutional Protection

Such a supposedly restricted right to privacy has received the utmost priority from Indian courts, who believe that it may only be curtailed for compelling grounds like public safety and national security.⁶ Although a challenge was accepted in 2015, the Apex Court of India has decided in 2018 that the right to privacy is, definitively, a basic right protected by the Constitution.⁷ It is important to remember that the privacy of humans has been acknowledged as a basic right and is protected by several international human rights agreements.⁸

2. Information Technology Act, 2002 and Privacy Rules

The IT Act aims to safeguard electronic data, including non-electronic documents and information that have been, are being, or will be handled electronically. It contains relevant provisions for collecting, transferring and using personal data. According to the Privacy Rules⁹, businesses that collect, handle, and store personal data should be monitored to check if they properly follow rules regarding such handling of our data including sensitive personal information. As a subset of personal information, it differentiates between "personal information" & "sensitive personal data or information" ("SPDI").

⁵ Justice A. P. Shah, *Report of the Group of Experts on Privacy*, Planning Commission of India (2012), <https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf>

⁶ *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.

⁷ *Puttaswamy v. Union of India*, (2017) 10 SCC 1.

⁸ G.A. Res. 217 (III) A, Universal Declaration of Human Rights (1948).

⁹ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, MINISTRY OF COMMUN. & INFO. TECH., GOV'T OF INDIA, <http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>

Advertisement Targeting: A Seeming Attack On Data Privacy

3. Indian Contract Act, 1872

Under the Contract Act, one can get damages or compensation for the violation of any terms under the contract which may include one's privacy and also for not performing the promise made under the contract, including those which are connected to data expressly or not obligating the rules by breach of contract.

4. Criminal Laws – Indian Penal Code, 1860

Theft, misappropriation of property, and criminal breach of trust are all crimes that can be prosecuted in cases when data is stolen. For instance, the dishonest theft or conversion of another person's "movable property" for one's use is punishable by law under section 403 of the IPC.¹⁰ The penalty for such criminal violations, like a breach of trust, is severe and includes a fine, a term of imprisonment up to 3 years, or both.

5. Intellectual Property Laws – Copyright Act, 1957

Rights in literary, theatrical, musical, artistic, and cinematic works are governed by the Copyright Act of 1957 in India. In accordance with this Act, Indian courts have recognised the copyright in computer databases¹¹ & given them the status of "literary work." Depending on the seriousness of the offence, the Indian Copyright Act imposes obligatory penalties for copyright violations. According to Section 63B of the Indian Copyright Act, anybody found guilty of intentionally making an illegal copy of a computer program by using a computer faces a minimum jail sentence of 6 months and a maximum sentence of 3 years.

6. Credit Information Companies Regulation Act, 2005

The Credit Information Companies Regulation Act ("CICRA") has established a stringent framework for safeguarding information on the credit and finances of individuals and businesses in India. It is based on the Fair Credit Reporting Act and Graham Leach Bliley Act. The CICRA mandates that the credit information of Indian citizens be gathered in accordance with the privacy standards outlined in the CICRA rule. Regulations under CICRA, which have been announced by the Reserve Bank of India, set forth strong data privacy norms.¹² Any potential breach or change of this data is the responsibility of the organisations collecting and storing it. The following organisations are listed in the regulations as "specified users" who fall under the jurisdiction of the CICRA and are permitted to gather credit information.¹³

¹⁰ INDIAN PENAL CODE, 1860, §403.

¹¹ Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber, (1996) 113 PLR 31.

¹² Credit Information Companies Regulations, 2006 Under Section 37 of the Credit Information Companies (Regulation) Act, 2005, MINISTRY OF FINANCE, DEPT. OF ECONOMIC AFFAIRS, BANKING DIVISION, GOV'T OF INDIA, <https://rbidocs.rbi.org.in/rdocs/Content/PDFs/69700.pdf>

Advertisement Targeting: A Seeming Attack On Data Privacy

V. THE NEED FOR DATA PRIVACY LAWS

It is extremely essential to pass a particular privacy and data protection law as a starting point. So that it is not necessary to control private companies like Facebook or Google. It basically claims that if the consumer is having or is concerned with the issue of privacy while using any particular application then he/she will change their behaviour towards the application. These changes could be restricted use of the application or stopping the use altogether etc. such changes in consumer behaviour would drive businesses to provide better privacy safeguards. Users frequently have less knowledge than data controllers regarding the scope of data collection, how it is processed, shared, and used, as well as the implications of sharing this data with others or incorporating it into an algorithm.¹⁴ This is known as information asymmetry. In reality, consumers rarely receive any kind of notification when and if their information is shared with other parties. Researchers have discovered that consumers frequently consider privacy policies as promises of data protection, rather than just liability disclaimers for businesses, or that the mere existence of a privacy policy, independent of its contents, is viewed by the general public as a substantial privacy safeguard.¹⁵

The 2018 Draft Data Protection Bill, which was suggested by the Committee of Experts led by Justice Srikrishna, is a positive development. Taking into consideration international trends like the implementation of the “European Union General Data Protection Regulation (GDPR)” as well as the Supreme Court's “privacy ruling in Puttaswamy”, it has participated in public dialogue and aided in the advancement of the discussion on privacy and data protection.¹⁶ The cloud method is increasingly being seen by EU legislation as a “method reasonably expected to be utilised” and as making more information “identifiable”. In

¹³ *Id*, Rule 3.

¹⁴ Acquisti, Alessandro and Jens Grossklags, 'What Can Behavioral Economics Teach Us about Privacy', *Digital Privacy: Theory, Technologies & Practices*, 2007, Pp.363.

¹⁵ Tene, Omer and Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, Stanford Law Review Online, 2012, 65.

¹⁶ Vrinda Bhandari, *PRIVACY CONCERNS IN THE AGE OF SOCIAL MEDIA*, India International Centre Quarterly, Vol. 45, No. 3/4, Social Media in a Networked World (Winter 2018-Spring 2019), pp. 78.

addition, different dangers are connected to data that may be linked to an identifiable person rather than information that is currently attached to an identified person.¹⁷

While in India, in *People's Union for Civil Liberties v. Union of India*¹⁸, the Supreme Court noted that data sharing promotes the right to knowledge of a voter or citizen. The right to privacy of an individual must be given priority over the right of people to information when their interests conflict because the former serves a greater good. The issue of a voter's right to know about a candidate's privacy is raised. It calls for a balanced interest and attitude. Therefore, communal good and individual liberty must finally have a healthy and cordial connection.¹⁹

VI. CONCLUSION

The issue of implementation comes first. India has a limited state capacity, as seen by its poor ability to enact effective laws and enforce them. To ensure the effectiveness of the laws, certain things need to be ensured. Firstly, the grievance redressal method must be efficient and user-friendly. The capacity to guarantee the Data Protection Authority's (or any other ombudsman's) financial and functional independence, which is planned to be established under the Draft Bill of 2018, must be second and related. The third more significant concern should be about how the laws may unintentionally strengthen the monopoly of current firms by making it more difficult for new competitors to enter the market.²⁰ When evaluating the effects of the loss of our privacy caused by actions taken by the government as well as private entities, all these elements need to be taken into consideration. In the world we live in, technology will always advance faster than the law. Today, big data has given the government and commercial businesses the ability to build detailed profiles of citizens and individuals, giving them tremendous power to conduct surveillance or make important choices that directly affect people's lives.²¹ Through the public discussion of the Srikrishna Committee Report and the 2018 draught Data Protection Bill, we as a nation have moved in the right direction towards ensuring a more secure and less restrictive digital world.

¹⁷ Schwartz & Solove, Council Directive 95/46, at 1841-45 (explaining how individuals can be re-identified by putting together various pieces of de-identified information).

¹⁸ AIR 2003 SC 2363

¹⁹ Shiv Shankar Singh, PRIVACY AND DATA PROTECTION IN INDIA: A CRITICAL ASSESSMENT, *Journal of the Indian Law Institute*, October-December 2011, Vol. 53, No. 4, pp. 670.

²⁰ Supra note 12.

²¹ *Id.*, at 79.