Volume 17, November 2021 ISSN 2581-5504

"The Threat to our Personal Data"

**Sriharsha Ravi Madichetty*
Jindal Global Law School

***Shresth Goel*
Jindal Global Law School

ABSTRACT

In a society, we have laws to govern us. In that sense we have various acts and laws enacted by the Indian legislature which contain provisions that tell us what is legal and what is illegal and the consequences if we try to go against the law. As time goes by, the society changes and we have to change with time along with the laws which would be appropriate to the environment and society we live in., and the parliament has strengthened these laws by way of amendments or by enacting new laws. We live in a world where data and privacy are the most important aspects in our daily lives. Particularly the 21st century has seen digitalization at an exponential rate. This paper focus on the data protection laws in India, the need for new data protection laws vis a vis the personal data protection bill, 2019 and explores the drawbacks and flaws with regards to the bill.

INTRODUCTION

The twenty first century has witnessed extensive digitalization where most of the daily activities have been replaced by digital portals. Especially in the year 2020 where the world went more digital than ever before and one of the silver linings of the year was the spotlight on the importance of data and data flow.[1] In the contemporary world, the most crucial aspect of every individual is their personal data which can be described as any information that is related to identifying or linked to the identity of an individual. This data constitutes information such as name, phone number, medical records, credit/debit card details, internet protocol (IP) address etc. The use of internet plays a vital role by supporting all the industries and sectors ranging from small businesses to multinational corporations.

In 2020, India had nearly 700 million internet users across the country and this figure was projected to grow to over 974 million users by 2025[2]. Daily, each user visits various web applications and unknowingly grants access to their personal data, but they do not remember giving such permissions. The answer lies in the terms and conditions with respect to the privacy policy of the website. People generally ignore these pages and end up clicking on "I agree to all

[1] Purushotham Kittane, Privacy and Data Protection – India Wrap 2020 The National Law Review (2021), https://www.natlawreview.com/article/privacy-and-data-protection-india-wrap-2020
[2] Sandhya keelery, Total internet users in India | Statista Statista (2021), https://www.statista.com/statistics/255146/number-of-internet-users-in-india/

the terms and conditions".[3] By doing so, they are unknowingly granting access to their personal data such as contacts, location and media that are stored on their device to these web applications. Granting access to personal data is not the problem here, but it arises when this data is stolen by cybercriminals, or the data is misused by the web applications to whom the access is provided to.

The worldwide outrage for a strong data protection law can be heard from the major "The Cambridge Analytica Scandal" happened in US where "*The firm in 2016 during the US Elections was accused of having access of the data of over 50 million Facebook users without their consent, to analyze and lay predictions based on such data, which led to a trial in the year 2018."* [4] This research paper explores about various applications and threats associated with personal data and describes the laws governing the aspect of personal data protection in India.

"The IT Act is mainly aimed at e-commerce and e-governance. India doesn't have a dedicated cyber security law." - cyber law expert Pawan Duggal [5]

EXAMPLES:

Aadhar:

There have been instances in the past where the confidential data of Indian citizens was leaked and was openly available on government official websites. Aadhaar has always been into the controversy where the data protection on electronic database is considered as a national concern. Issued by the Unique Identification Authority of India (UIDAI), it considers biometric details and demographic information.[6] The World Economic Forum's Global Risks Report 2019, says, "The largest (data breach) was in India, where the government ID database, Aadhaar, reportedly suffered multiple breaches that potentially compromised the records of all 1.1 billion registered citizens. It was reported in January 2018 that criminals were selling access to the database at a rate of Rs. 500 for 10 minutes. [7] Along with identity thefts, there are other serious concerns like illegal tracking of individuals. Also, Aadhaar does not record the purpose of authentication.

[3] PERSONAL DATA PROTECTION LAW IN INDIA, Legal 500 (2020), https://www.legal500.com/developments/thought-leadership/personal-data-protection-law-in-india/

[4] Cambridge Analytica and Facebook: The Scandal and the Fallout So Far (Published 2018), Nytimes.com, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[5] Satya Prakash, Information Technology legislation 'falls far short' Tribuneindia News Service (2021), https://www.tribuneindia.com/news/features/information-technology-legislation- 'falls-far-short'-21652

[6] Aadhaar card guide: What is Aadhaar Card? Everything you need to know about Aadhaar, The Economic Times (2020), https://economictimes.indiatimes.com/wealth/personal-finance-news/aadhaar-everything-you-need-to-know-about-it/articleshow/60173210.cms?from=mdr

[7] Yogesh Sapkale, Aadhaar Data Breach Largest in the World, Says WEF's Global Risk Report and Avast MONEY LIFE (2019), https://www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html

Volume 17, November 2021 ISSN 2581-5504

Authentication without authorization and accounting puts users at serious risks of fraud because authentication or KYC meant for one purpose may be used for another.[8]

The personal data can also be misused by the electoral parties attacking the very essence of Indian Democracy. This can be used by a political party to advertise and influence the citizens like in the case of Cambridge Analytical where a psychological warfare tool was created to help Donald Trump win the Presidential Elections. Similar instances were observed in India but did not gain much light where the personal date of Indian users was stolen and later transferred to an outside source.[9] Christopher Wylie, who exposed Cambridge Analytica's role in a data breach tweeted documents that suggested the firm's parent company, Strategic Communications Limited (SCL), conducted behavioral research and polling for at least six state elections in India between 2003 and 2012, including the 2009 national election.

The WhatsApp privacy policy controversy:

At the beginning of 2020, WhatsApp has announced an update to its privacy policy, which sparked huge controversy concerning data protection issues. As per the update- the app will be able to share user information such as phone numbers and transaction data after the amended privacy policy is accepted[10]. Additionally, photographs and the contents of some conversations will now be automatically shared with Facebook under the new policy. This is where the concern began since the parent company of WhatsApp, i.e., Facebook is involved which has a history of misusing user data along with many past incidents of data breach.[11] WhatsApp and the Facebook family of companies may both use the information to help operate, provide, enhance, understand, customize, support, and promote their Services and their offerings.[12] Due to weak data protection laws in India, there is no proper regulation of how the citizens' data is being used or sent somewhere without their consent.

[8] PTI. UIDAI suspends Airtel, Airtel Payments Bank's e-KYC license over Aadhaar misuse, 2017; http://bit.ly/2IJnjdR

[9] Amit Kumar Chaudhary, Exposed: India's own Cambridge Analyticas stealing voter data India Today (2018), https://www.indiatoday.in/india/story/exposed-india-s-own-cambridge-analyticas-stealing-voter-data-1223403-2018-04-30

[10] Jagmeet Singh, WhatsApp Privacy Policy Update: What Happens When You Don't Accept? NDTV Gadgets 360 (2021), https://gadgets.ndtv.com/apps/news/whatsapp-privacy-policy-update-changes-what-happens-if-you-dont-agree-details-facebook-data-2376020

[11] WhatsApp controversy highlights growing fears about data privacy | DW | 18.01.2021, DW.COM, https://www.dw.com/en/whatsapp-controversy-highlights-growing-fears-about-data-privacy/a-56266093

[12] Blake Morgan, WhatsApp Controversy Shows Just How Much Privacy Matters to Customers Forbes, https://www.forbes.com/sites/blakemorgan/2021/01/14/whatsapp-controversy-shows-just-how-much-privacy-matters-to-customers/

Volume 17, November 2021 ISSN 2581-5504

Chinese apps:

The banning of Chinese apps in India looks like a purely political move but the actual reason behind was the data protection. These Chinese apps asked the users permission to access different information where they did not know why it was asking for such permissions and grant permissions without knowing what they are giving access to. Some of the data sought was IMSI, IMEI, SMS and text message access, and many more. With IMSI, one can monitor across several devices, cybercriminals are interested in data such as the IMSI or IMEI as they can obtain sensitive information from them. They could use it to report the phone as stolen, causing the provider to disable the device and prevent its network access and intercept phone calls.[13]

UC Browser has numerous issues of downloading malware programs that perform a variety of nefarious operations. The browser prompts you for needless permissions, such as access to your text messages, when you first launch it. Consider how incorrect this is in the case of sensitive OTPs and other bank-related data. UC Browser also downloads dangerous files and material in the background on your device without your knowledge.[14] TikTok has been at the vanguard of the global ban on Chinese apps. "TikTok is essentially malware" and "TikTok is a data harvesting service that is thinly masked as a social network." [15]It's not just the worry of unknown surveillance dangers, but also other cybercrimes such as stolen TikTok user accounts, gathering sensitive data without permission, and other data breaches.

INDIAN PRIVACY CODE:

To make the laws stronger and effective, it is important to consider the seven privacy principles of the Indian Privacy Code, 2018. These principles give a glimpse of Indian Privacy Code and are a result of #SaveOurPrivacy campaign where experts drew several codes and globally accepted practices that can be adapted in Indian dynamic conditions. The first principle talks about the induvial rights and is based upon the idea that in order to promote innovation in a sustainable way, the requirement of data protection law is essential. The second principle upon which the Privacy Code is based is that while framing data protection laws, due consideration must be given to the core Principles of Privacy. This includes the rights given by the Justice A.P. Shah Committee of Experts, Supreme Court's decisions and the European Union's General Data Protection Regulation to adopt globally accepted guidelines. The third Privacy Principle highlights a major need of Commission which should be created to enforce the Privacy

[13] Richi Jennings, Google Finally Pulls Chinese Apps Stealing Personal Data Security Boulevard (2020), https://securityboulevard.com/2020/11/google-finally-pulls-chinese-apps-stealing-personal-data/

[14] Mishka Grey, How TIKTOK & Other Chinese Apps Are Stealing Your Data Hack Reports (2020), https://news.hackreports.com/tiktok-ban-chinese-apps-stealing-data/

[15] GAVIN PHILLIPS, Are TikTok and Other Chinese Apps Really Stealing Your Data? MUO (2020), https://www.makeuseof.com/tiktok-chinese-apps-stealing-data/

Volume 17, November 2021 ISSN 2581-5504

Principles and keep a track over them. This body with wide powers of investigation, adjudication and enforcement keeps a potential to bring more accountability in the system. Another major advantage the commission can serve is the power to make new rules with advancement of new technology, this way the commission can update the code to meet new requirements. Despite having courts, the Code provides another redressal mechanism where the grievances can be herd, and this comes again within the purview of the Powers of Privacy Commission who can hold and pass appropriate orders. The fourth principle on focus discusses the Governments' response to the user privacy. Even the most powerful body should respect the privacy, and nothing is above the public benefit, it is important to give privilege to the fundamental rights. Under Privacy commission, the government can also be made accountable just like a private sector and government cannot ask or coerce the citizens to share the data to enjoy essential services and benefits provided by the government. The fifth principle brings the need of proper surveillance reform. It focuses on the indiscriminate mass surveillance done by government and there should be some limits over it to make it proportional. There is a need to avoid illegal collection of evidence where a clear absence of valid tapping orders is observed. To ensure the credibility and accountability of such orders it becomes important to communicate the information to the surveilled person. The sixth major principle observed talks about the Right to Information, which needs to be strengthened in the sense that information commissioners should be exempted from the control by privacy commissioners to maintain their independence. The last principle followed by the Code acknowledges International Protections. With open access to internet worldwide it becomes important to incorporate services which are outside the territory of India but are accessible in India and stores the personal data of Indian citizens. This should be done in a very cautious way without undermining the protocols and advantages of global open internet services like web series. [16] These were the seven privacy principles which should be incorporated while framing Data Protection Laws in India so that the advancement and adoption of technology happens in a more sustainable, fair and legal method.

PERSONAL DATA PROTECTION BILL, 2019:

Data principals[17]: personal data of individuals

Data fiduciaries[18]: data processed by entities

Mr. Ravi Shankar Prasad, Minister of Electronics and Information Technology, introduced the Personal Data Protection Bill, 2019, in Lok Sabha on December 11, 2019. The Bill aims to protect individuals' personal data and establishes a Data Protection Authority in India. The Bill proposes to repeal Section 43-A of the Information Technology Act of 2000 by removing the provisions relating to compensation payable by entities for failure to secure personal data of an

[16] Save Our Privacy | 7 principles of the Indian Privacy Code, Save Our Privacy, https://saveourprivacy.in/principles
[17] Section 14
[18] Section 13

Volume 17, November 2021 ISSN 2581-5504

individual. It specifies how personal data should be collected, processed, used, disclosed, kept, and transferred[19].

Applicability of the bill:

Personal data is information about an individual's qualities, traits, or attributes of identification that can be used to identify them. The Bill regulates the processing of personal data and would apply to the personal data collected, disclosed, shared, or otherwise processed within the Indian territory by the government, Indian companies, and foreign companies dealing with personal data of Indian citizens. Certain personal data such as biometric information, caste, religion, financial information, or political opinions is classified as sensitive personal data under the bill. At the same time the bill shall not apply to the data categorized as non-personal or anonymized data to help the government delivery of its various services and policies[20].

Consent of the data principal:

As per the bill, the personal data will be processed only after obtaining the consent of the individual. However, there is a provision where the consent is not required in circumstances such as legal proceedings against the individual, for medical emergency, for the government to provide services and various benefits to the individual through its various policies.

Issues with the bill:

As per the bill, a data fiduciary is obligated to inform the data protection authority that will be set up under this bill regarding any breach of personal data whenever such a breach might cause harm to the data principal[21]. This might look like a provision that is included to protect the interests and data of the data principals. But there is a possibility where a data fiduciary might not report such breaches so that they can protect their public image and reputation. Popular example for this would be in 2019 where American cybersecurity giant Symantec underreported a data breach that gave a hacker access to passwords and a list of the company's clients, which included significant government institutions[22]. The company cited that this is fairy a minor data breach but in reality, it significantly affected the company's clients on a global level.

The bill states that a private company needs to obtain the consent of the data principal in order to process their personal data. But this restriction does not apply to the state where they don't need

[19] Angelina Talukdar, Key Features of The Personal Data Protection Bill, 2019 - Privacy - India Mondaq.com (2020), https://www.mondaq.com/india/data-protection/904330/key-features-of-the-personal-data-protection-bill-2019

[20] Section 91 (2:)

[21] Bill: Clause25(1)

[22] Paul Karp, Cybersecurity giant Symantec plays down unreported breach of test data the Guardian (2019), https://www.theguardian.com/technology/2019/jun/14/cybersecurity-giant-symantec-plays-down-unreported-breach-of-test-data

Volume 17, November 2021 ISSN 2581-5504

to obtain the consent of the data principal for using their personal data if the purpose is to providing services through various government policies and programs. Even though this provision protects the data principals from misuse of their personal data by the private companies, it still leaves a lot of area for the government to use the data at their discretion.

The bill states that the personal data of the data principal can be transferred abroad but always a copy of the same should be stored in India[23]. The upside of storing such data locally would be faster access to data by police and other law enforcement authorities. But there is also a huge downside for storing personal data locally such additional infrastructure costs associated with storing the personal data locally within the country, due to the existence of such rule foreign entities will be forced to adhere to such rule and might back out from investing in India.

COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS

A comparative analysis of proposed bill with international data protection laws becomes necessary to strengthen the much-needed act. For this purpose, existing data protection laws in countries like Australia, Canada and European Union will be compared with the proposed 2019 Bill. Under section 28(3) and 28(4), the Indian personal data protection bill talks about social media intermediaries and directs them to provide a verification mark to registered Indian users who voluntarily verify their account as per procedure laid down by the government, this specific provision regarding these intermediaries is absent in the other jurisdictions. The list of categories that can be termed as sensitive data under international laws like GDPR is finite and specific but the Indian 2019 bill not only includes additional information such as financial data within this ambit but also grants the government this power to widen the scope of sensitive personal data under this definition. What further differentiates it from global laws is the imprisonment term, where most of the jurisdictions only penalizes with fine, under the Indian bill, the wrong doer can be imprisoned for a period up to a period of three years. Certain additional rights can be observed in the European Union's GDPR which are absent in the proposed Indian legislation, for example- the ‘right to object’ which enables the individual to object to processing of their data for profiling or direct marketing purposes, a much narrower version of it can be seen in the form of right to be forgotten in PDPB.[24] Comparing with multiple jurisdictions, the laws in Canada and the European Union do no mandate the local storage of data, whereas the Australian jurisdiction mandates some specific sectors like local storage of health data. The Indian bill on the other hand makes it mandatory to store a local copy of sensitive personal data. There are certain exemptions which can be seen in all the four jurisdictions where the GDPR and Australian law stands almost same by providing exemptions broadly for defense, judiciary and journalistic purposes etc. The Canadian jurisdiction do not give such blanket exemptions, only

[23] Bill: Clause33(1)

[24] The Personal Data Protection Bill, 2019, PRS Legislative Research, https://prsindia.org/billtrack/the-personal-data-protection-bill-2019

for journalistic purpose such relaxations can be granted by taking consent. While the proposed Indian bill provide massive exemptions for Sovereignty and integrity, national security, friendly relations, public order, prevention and prosecution of offences, research and journalistic purpose, where the terms sovereignty & integrity and public order can be called vague and possibly further misused by the concerned authorities. [25]This comparative analysis shows that even though the proposed bill is similar in many ways, but it can be distinguished on many factors.

CONCLUSION

The COVID 19 pandemic has had a significant impact on our perceptions of privacy and the value we place on the protection of our personal data[26]. The stealing and usage of personal data without consent has become a common practice in India which has shown to have negative consequences for the owner of the data.

Forbes reported that about 2.5 quintillion bytes of data are generated every day, and this staggering figure is only going to rise[27]. Collecting data of customers can help improve almost any aspect of the business and you want to ensure that the data is used in best possible way, regardless of industry in which you work, the demographics in your target market or the type of services you provide[28].

But if such data is misused then the public at large will lose confidence in companies to trust them with their data. Furthermore, they would lose trust in the government if stronger data protection laws were not enacted. The personal data protection bill was introduced in the parliament in 2019. Meanwhile the pandemic has started, and the bill is yet to be passed. Data protection laws are crucial because they provide organizations and the government with directions and best practices on how to use personal data. But if proper laws are not enacted then it creates a loophole in our justice system and indirectly provides freedom to national and multinational corporations to misuse the personal data of citizens. We should realize that the realm of internet is sensitive and the data that flows through it is very important, and we have to make sure it is protected. Hence stronger Data Protection laws are the need of the hour in India!

[25] Id

[26] Emanuele Ventrella, Privacy in emergency circumstances: data protection and the COVID-19 pandemic Springer Link (2020), https://link.springer.com/article/10.1007/s12027-020-00629-3

[27] Bernard Marr, How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read Forbes (2018), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=2825ca0260ba

[28] The Importance of Data: The Top Benefits of Collecting Customer Data, Insights.truyo.com, https://insights.truyo.com/consumer-data