THE RIGHT TO PRIVACY IN THE DIGITAL AGE: HOW TECHNOLOGY IS IMPACTING PRIVACY ON SOCIAL MEDIA

Ayushman Patnaik and Harshit Arora, BA.LLB, Department of Law, Maharaja Agrasen Institute of Management Studies affiliated to GGSIPU

ABSTRACT

This article addresses the need and relevance of privacy laws universally. It discusses how the meaning of privacy is interpreted with respect to social media, as well as users' understanding of privacy laws and regulations in the digital era. In light of increased public awareness regarding privacy debates, this article examines how users interpret privacy as a legal issue in the form of internet breaches, stalking and threats, as well as how they negotiate their web activity, especially on social media sites. This article reviews how the definition of personal privacy has evolved, as well as how today's legal standards are insufficient in our digital and social media world. It examines the interests and understanding of individuals with respect to privacy, which is widely recognised as a matter of protecting one's data, including the disclosure of information even to friends, and is closely linked to concerns of individual freedom. And how a simple thing like in today's world people utilise numerous social networking platforms for a variety of reasons. Nonetheless, if your password is insecure, your account's security is jeopardised. This article further explores the potential and the technical aspects of the upcoming Indian Personal Data Protection Bill 2019. The proposed regimes under the Personal Data Protection Bill are projected to be far more robust in safeguarding data than present systems, which are incapable of adequately securing data. The major theme of this article is how the Personal Data Protection Bill would remodel and enhance the present data protection legal system.

Keywords: Social media sites, digital era, privacy, internet breaches, personal data protection bill

INTRODUCTION

Since the early 2000s, when the first social media sites were introduced, many online social media users have grown steadily, with Facebook, YouTube, Twitter, and WhatsApp being the most popular in this digital era. Although, the legality, knowledge, and limits of potential privacy breaches are pivotal issues in advance of the modern world, the extent to which people and social media network operators can control or exploit user profiles has recently become a topic of ethical debate.[1]

In general terms, privacy can be interpreted as "the condition or the state of being free from public attention to intrusion into or interference with one's acts or decisions"[2] and digital privacy refers to safeguarding an individual's data when accessing the internet on a computer or mobile device. In our ever-evolving, technology-based, modern world privacy is both a critical and contentious issue, and it can have a significant effect on public relations practice for public relations practitioners. Advances in information technology have prompted questions about data protection and its consequences, leading Information Systems experts to investigate these problems and technological ways to solve them.[3]When content and data exchanged on the social network has been increasingly commercialized, social-media consumers are now called unpaid 'internet labors,' as one pays for 'free' e-services by sacrificing their anonymity.[4]

Now, what is social media and why has it become a hot topic in recent times? Social media is a tool that Individuals use as an online means of communication to exchange information with relevant parties (friends, colleagues, customers, etc.). People actively follow anyone who shares content through social media platforms such as Twitter, Instagram, Snapchat, and Facebook. Social media is getting more prevalent these days as a result of its user-friendly functions. Via social media websites such as Instagram, Snapchat, Facebook, people would be able to chat with each other irrespective of the other persons' location. These social networks' main goal is to create intelligence in the physical world. To put it another way, social media

[1] Mircea Turculeţ, "Ethical Issues Concerning Online Social Networks"*, Procedia - Social and Behavioural Sciences"*, Volume 149, 2014, pp. 967-972
[2]Black's Law Dictionary 1315, 9TH ED., 2009
[3] Bélanger, France, and Robert E. Crossler, "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems*." MIS Quarterly*, Volume 35, 2011,p. 4,
[4] Trebor Scholz, **"**The Internet as Playground and Factory*",Digital Labor Taylor & Francis* (ed.), 2012

has brought the entire world to our fingertips. However, few people were aware that this boon was also linked to the crime.

The expansion of privacy law standards to advanced media was critical, given how much data was stored in digital form and how easily it could be shared and uncovered. Furthermore, recent trends have seen an increase in the number of individuals and corporations carrying vast amounts of data for different purposes.[5]"With dossiers being compiled by bureaus, state and local law enforcement departments, the CIA, FBI, IRS, the Armed Forces, and Census Bureau, we live in an Orwellian era in which Machine has become "heart of monitoring system that will transform society into a transparent world," stated Justice Douglas in the case of Sampson v. Murray[6].

LAWS & REGULATIONS SAFEGUARDING INDIVIDUAL'S DIGITAL PRIVACY

Contrary to Indian society's communal notions, courts have frequently addressed several facets of the right to privacy. Due to the absence of a general statute guaranteeing the right to privacy, this was required. Though other countries may follow India's lead, India was one of the few countries until recently that did not have any technology-specific laws.

The Indian legislature only realised the ever-expanding scope of the internet in 2000 (Information Technology Act, 2000), and it has been trying to gain on ever since. However, the privacy regulations were largely lacking in the Statute. It is apparent in a telling analogy of legislative lethargy that telecommunications interception regulations have only been framed in 1999 after the decision of the Supreme Court in PUCL v. Union of India[7]. These regulations lay the foundation for violating privacy rights of 'intrusion into the solitude or seclusion of a person' and 'information collection'. These rules reflect closely the rules recently enacted by Sections 69[8] and 69B[9]

Section 69 of the Information Technology Act, 2000

The Information Technology Act 2000 received its first major amendment in the year 2008

[5] Meenakshi Bains, "Right to Privacy in the Digital Era",*Amity International Journal of Law and Multidisciplinary Studies*, Volume II, Issue No. III, 2018
[6]1974 415 U.S. 61.
[7]*People's Union for Civil Liberties v. Union of India*, 1997 1 S.C.C. 301.
[8]*Information Technology Rules*, 2009, G. S. R. 780(E), Oct. 27, 2009.
[9]*Information Technology Rules*, 2009 G. S. R. 782(E), Oct. 27, 2009.

following great discontent and debate. The Amendment Act sought to correct the many shortcomings observed with the enactment's application.[10] The amendment sought to make the Information Technology Act, 2000 "a self-sufficient act with respect to internet behaviour"[11]. Hence the legislature set forth section 69. Section 69 is titled the "power to issue directions for interception or monitoring or decryption of any information through any computer resource." The section reflects section 5(2) of the Telegraph Act, that imposes the same restrictions on the use of the power to give orders. It has a similar structure that adheres to the constitutional limits set forth in PUCL[12], which states that a direction can be given only when:

(a) public emergency, or

(b) public safety situations exist.

It also contains the "requirement of recording reasons for issuing the direction" and mentioning the "5 classes of events" as contained in section 5(2). It is no surprise that the new regulations enacted under section 69(2) to provide a protocol for issuing directions broadly follow Rule 419-A. They reflect most procedural safeguards in respect of documentary adherence, supervision, and automatic expiration.

Information Procession

Although section 69B is a "hybrid between information gathering and processing", the layout is properly concerned with processing data.[13] The section is entitled "power to authorise to monitor or collect traffic data or information through any computer resource for cyber security." The objectives of the section are essential to improve internet management, with the specific mandate of "enhancing cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminants." To that end, the section enables the "traffic data or information generated, transmitted, received or stored in any computer resource to be monitored and collected." The harms that will be incurred are in the essence of information processing, such as aggregation and identification, according to a summary of the regulations created under the provision.[14] While the section includes similar safeguards to section 69, the

[10] *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*, United Nations 1999.
[11] *Information Technology (Amendment) Act*, 2008, No. 10 of 2009.
[12] *Supra* note 7.
[13] *Information Technology Act*, 2000, No. 21 of 2000, s 69B.
[14] *Information Technology Rules*, 2009 Rule 3(4).

circumstances in which the power is exercised are entirely different. As a result, the explanations that must be documented do not meet Section 69's stringent requirements. These are the reasons that have been mentioned in the PUCL case. As a result, there is a case to be made that the section is unconstitutional since the regulations imposed under it specifically envision separate directions to track data, which necessitates interception as a technical requirement.

INDIAN CONSTITUION AND PRIVACY

The Supreme Court of India has recognised the Right to Privacy as a "subset of the larger right to life and personal liberty under Article 21 of the Indian Constitution" in several decisions.[15] The Article states, "no person shall be deprived of his life or personal liberty except according to procedure established by law". The Supreme Court of India has declared that Article 21 of the Indian Constitution is the foundation of Fundamental Rights. The expansion of Article 21's dimensions was made possible by giving the words "life" and "liberty" in Article 21 a broader meaning. The extent of this right was first discussed in the "Kharak Singh V. State of Uttar Pradesh case (Uppal, 2015)"[16] which was concerned with the legality of certain regulations that allowed for the surveillance of suspects.

The right to privacy was revisited by the Supreme Court in 1975 in the context of Article 19(1)(d). The Supreme Court while deciding the case of Govind v. State of Madhya Pradesh[17] laid down that "a number of fundamental rights of citizens can be described as contributing to the right to privacy." The Supreme Court did, however, state that the right to privacy would have to be developed on a case-by-case basis. In the case of R. Rajagopal v. State of Tamil Nadu, the Supreme Court for the first time directly linked the right to privacy to Article 21 of the Constitution. and laid down thus: "The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a 'right to be let alone'. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing, and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether

[15]*Kharak Singh v. State of UP*, AIR 1963 SC 1295; *People's Union of Civil Liberties v. The Union of India*, 1997 1 SCC 318.
[16]*Kharak Singh v. State of Uttar Pradesh*, 1964 SCR (1) 332.
[17]*Govind v. State of Madhya Pradesh*, AIR 1975 SC 1378

laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned[18] …"

The Fair Information Practice Principles (FIPP) are credited with popularising the concepts of privacy and data protection. International regimes such as the OCED Privacy Guidelines, the APEC Framework, and the nine National Privacy Principles articulated in the Justice A.P Shah Committee Report uphold these principles as well. In 2012, the Justice A. P. Shah panel proposed an overarching law to protect personal data and privacy in both the private and public spheres. The report also advocated for the establishment of "privacy commissioners at both the federal and state levels". It has outlined nine national privacy principles that could be used to propose legislation.[19] The Supreme Court stated that the right to privacy may be limited for the prevention of crime, disorder, or the protection of health or morals, or for the protection of others' rights and freedoms. Unfortunately, the Centre responded in the Supreme Court in July 2015, during the hearing of a batch of petitions seeking to halt the implementation of the Aadhaar Scheme, that privacy was not a fundamental right in India. Attorney-General Mukul Rohatgi stated that "the right to privacy has been a vague concept for many years, with varying Supreme Court conclusions". Individuals have the ability to consent under these frameworks, and they should be notified if their personal data is used and informed how it is being handled.

PRIVACY ON SOCIAL MEDIA HANDLES

Users' concerns over their privacy on social media have grown in recent years. Many people have become concerned about privacy leaks, urging them to rethink about their social network activities and the security of their private data. According to a recent report, approximately half of those surveyed prefer to keep their social media accounts secret, while the other half prefers to keep them public and free. Furthermore, many people keep social media profiles and the applications that go along with them as a convenience. A social media site is a social structure made up of a community of social entities (organizations or individuals), a series of social relations and other social connections.

Invasion of privacy on social media networks is caused by a number of causes. It has been recognized that "by default, social media platforms threaten systems for ownership and access

[18] *R. Rajagopal v. State of Tamil Nadu* 1994 SCC (6) 632
[19] Report of the Group of Experts on Privacy (2012)

to personal information," as the sharing of viewer information is critical to their function. This shows that for social networking sites to function, private information must be made public.[20]

So the real question before us is whether the individuals can protect their privacy on social media or not? Controlling your social media privacy is practically impossible. This is because your friends and family can share your personal details even though you do whatever you can to protect your privacy on social media, including deleting your account. In this situation, even deleting your social media platforms cannot be helpful. Because of the obvious lack of privacy on social media, it's important to safeguard your online privacy before sharing anything on any social media site.

DATA MARKETS

Personal data collected in online markets can be used for a variety of purposes, including providing and tailoring services, optimising business processes, building partnerships, lowering costs, enhancing risk analysis, market analysis, and advertising targeting. There is no single, centralised market for personal data, nor is there a single model for using that data. On the opposite, data is used as an asset in a variety of markets to create or increase value from sales. So, where does personal information for online services come from? They come from a variety of places to find service providers.

Source	**How are data collected by service providers?**
Direct Collection (including tracking)	Directly from individuals
Data brokers, other service providers	Indirectly, using commercial agreements for data selling/sharing

[20] Kelly Quinn, Why We Share: A Uses and Gratifications Approach to Privacy Regulation in Social Media Use*, Journal of Broadcasting & Electronic Media*, (2016) 60:1, 61-86

Public registries	Indirectly, either from registry or by means of a data broker
Third- party tracking	Indirectly, by means of a third party
Other publicly available services/ websites	Usually indirectly, by means of a 'voyeur' or data broker
Other users	Indirectly from other users (e.g. Tagging a friend in a picture)[21]

As there is so much information on the internet now, certain details can be deduced, including an individual's name and address, that can then be used for identity fraud. As a result, different organizations have urged users to either not display their phone number or conceal it from people they don't know.[22]

Preteens and early teenagers are perhaps the most common victims of private-information-sharing behaviour amongst all age groups. Many teens believe that digital networking sites and social media platforms are helpful in forming friendships and relationships, as per various reports. This aspect creates privacy concerns, like identity theft, data breaches, and advertising agencies exploiting private information. Teenagers use social media for more than just connecting; they also use it for political reasons and to gather information.[23]

[21] Marcin Betkier, *Privacy Online, Law and The Effective Regulation of Online Services,*Intersentia, (2019)
[22]Gross, Ralph & Acquisti, Alessandro Information revelation and privacy in online social networks (The Facebook Case). WPES'05: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. 71-80, (2005)
[23]Monica Anderson & Jingjing Jiang, Teens and their experiences on social media, available at <https://www.pewresearch.org/internet/2018/11/28/teens-and-their-experiences-on-social-media> (Accessed on Mar,20, 2021)

Phishing has become one of the most popular ways for hackers to access sensitive private data A phishing attack appears as a real message and is sent by an email, text message, or through a phone call. Such messages convince users to exchange private information including OTP's, financial accounts, or credit card details. Botnet attacks, on the other hand, have become more prevalent day by day. Social networking bots create posts or instantly follow new users when a single term is listed on social networking sites. A botnet is a set of bots connected together in a network. On social networking sites, bots and botnets are commonly used to steal information, install malware, and launch distributed denial-of-service (DDoS) attacks, which allow hackers to gain access to individual's devices and applications.[24]

Harm to Individual Values: Autonomy and Dignity

While the language of risk is useful for describing the economic dimension of privacy damage, it falls short of completely addressing other privacy values. This is due to the fact that lack of dignity or autonomy does not only pose a risk of potential negative consequences; it also has an immediate effect on individuals. This effect is manifested, for example, by a reduction in the ability to function independently (towards individual goals). It can be subtle at times, but it is always there, and it is generally linked to the negative effects mentioned in the previous section. Surveillance is a common concept used to describe large-scale data collection. The relationship between online service providers and data subjects can be compared to Bentham's Panopticon model of surveillance, which Foucault further developed. Data subjects, like in the panoptical prison, are identified and constantly visible, but they lack the ability to control how their data is used. The architecture of online services and asymmetrical views function exactly as predicted by Foucault – that is, as a disciplinary mechanism integrated into an economically efficient architectural structure that wields power over individuals. Individuals do not see the power, but they are constantly, pervasively, and finely regulated.[25]

These models demonstrate the violation of individual values by those conducting online surveillance of users. First, they point to the modification of individuals' behaviour against their wishes and the violation of their autonomy. Individuals who are disciplined, continuously regulated, 'reassembled and targeted,' or whose data is offered in the market of behavioural

[24]Blog-Tulane School of Professional Advancement's programs, Key Social Media Privacy Issues for 2020, available at<https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020> (Accessed on Mar,20, 2021)
[25]K. Yeung, "Hyper nudge": Big Data as a Mode of Regulation by Design'*Information, Communication & Society,* (2017)*,* 118 – 36, p. 131

control are deprived of the ability to act autonomously. This is due to the fact that service providers direct their actions. This results in a lack of autonomous actions, which was a common feature of the problems described in the preceding section: manipulation, coercion, and discrimination.

Autonomy is also infringed because of the mechanism called 'filter bubble', ' autonomy trap ',[26] or echo chamber, which is the result of placing individuals in an environment based on past data reflecting pre-existing beliefs and inclinations. Algorithms governing what is seen on social media or in search results, for example, contribute to the creation of such an environment. This deprives people of the elements of surprise and serendipity that help them learn and grow. This has an impact on their ability to generate new ideas because this ability is dependent on the freedom of thought and belief, the freedom to engage in intellectual exploration, and the confidentiality of communications with others.[27]

DATA BREACHES OVER THE YEARS

A few years ago, a data breach affecting a few million users would have made headlines. Breach affecting hundreds of millions or even billions of people is all too common these days. In the first two of the century's top 15 data hacks, around 3.5 billion individuals' sensitive information was hacked. Some of the major data breaches are-

- **LinkedIn (2012 & 2016)**

Details: Since LinkedIn is the most common social media platform for industry professionals, it is becoming an appealing target for hackers seeking to carry out cyberattacks. The IDs were allegedly obtained from a four-year-old data breach, which was previously believed to have only involved a fraction of that amount. The industry-focused networking site said at the time that it had reset the profiles of those it believed had been hacked.[28]

- **Adobe (2013)**

Details: In early October 2013, Adobe revealed that cybercriminals had stolen 3 million

[26]T. Zarsky, '"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion' *Yale Journal of Law & Technology*(2002) 5, 1, p. 35
[27]N.M. Richards, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, *Oxford University Press, Oxford*(2015), p. 108
[28]BBC News Services,Millions of hacked LinkedIn IDs advertised 'for sale', available at<https://www.bbc.com/news/technology-36320322> (Accessed on Mar,27, 2021)

encrypted consumer credit card numbers, as well as login details for an undisclosed number of user profiles. Since some of the folders on the hackers' server that contained the stolen source were password secured, it was difficult to completely inspect some of the data, and Adobe was hesitant to comment on the number of people that may have been affected.[29]

- **eBay (2014)**

Details: In May 2014, eBay announced that a hacker exposed the account information of 145 million users. In a cyberattack which occurred in late February and early March, unknown hackers accessed emails, encrypted codes, birth dates, mailing addresses, and other private info. Financial information was not included in the data that was compromised. eBay's PayPal payments division, which encrypts and secures the records, showed no evidence of unauthorized access to financial or payment details, as per the company.[30]

- **Yahoo (2013-14)**

Details: In September 2016, Yahoo announced that it had been the victim of the biggest data attack in history in 2014. The hackers obtained access to 500 million users' real names, mailing addresses, dates of birth, and contact information, which the organization considered to be "state-sponsored actors." According to Yahoo, the rest of the passwords that were exposed were hashed. As per the company, the leaked information did not contain simple text passwords, card payment details, or bank account information. The data was encrypted with outdated, easy-to-crack cryptography, according to academic experts.[31]

- **Dubsmash (2018)**

Details: In December 2018, Dubsmash, a video chat service headquartered in New York, had 162 million addresses, usernames, PBKDF2 passwords, and other private information such as date of birth was compromised, and everything was then traded on the Dream Market dark web

[29]Brian Krebs, Adobe Breach Impacted at Least 38 Million Users, available at<https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users>(Accessed on Mar,27, 2021)

[30]Jim Finkle, Soham Chatterjee & Lehar Maan,EBay asks 145 million users to change passwords after cyber-attack, available at <https://www.reuters.com/article/us-ebay-password idUSBREA4K0B420140521>(Accessed on Mar,27, 2021),

[31]All 3 billion accounts hacked in 2013 data theft: Yahoo, Reuters, available at <https://economictimes.indiatimes.com/tech/internet/all-3-billion-accounts-hacked-in-2013-data-theft-yahoo/articleshow/60932776.cms>(Accessed on Mar 27, 2021)

market the following December[32]. Some of the apps, according to sources, use old password authentication techniques and the PostgreSQL database software on the backend. The value of using two-factor authentication, checking for alerts on a daily basis, and using complicated passwords is highlighted by this breach.[33]

- **Google (2018)**

After discovering a bug in a Google+ API that gave developers access to information classified as personal, the search giant announced in October 2018 that it would shut down its social media network Google+. According to sources and people informed about the incident, between 2015 and March 2018, a technical bug in the social media platform gave unknown programmers possible access to personal Google+ profile info, which was found and patched by internal investigators[34]. Google claims it has no proof that the information was misused or that Google+ was hacked during that time. Then, Google LLC settled a consumer class action case for $7.5 million over privacy leaks caused by two security flaws in the Google+ platform.[35]

- **Facebook (2019)**

2/3rd Facebook app datasets were found to have been leaked to the public Internet in April 2019. One, from Mexico's Cultura Colectiva, is 146 gigabytes in size and includes over 540 million records, comprising comments, likes, responses, account names, Facebook IDs, and much more[36]. Given the possible uses of such information, this type of collection, in a similarly concentrated form, has been a matter of concern in the recent past. The database was available for sale for $99 on another website in March, as per the posts. Several specialists, namely Alon

[32]Aziz Soomro, List of Biggest Information / Cyber Breaches of this century,available at <https://www.linkedin.com/pulse/list-biggest-information-cyber-breaches-century-aziz-soomro-lutcf>(Accessed on Mar,27, 2021)
[33]RSI Security, 10 OF THE LARGEST DATA BREACHES IN 2019, available at<https://blog.rsisecurity.com/10-of-the-largest-data-breaches-in-2019/> (Accessed on Mar,27, 2021)
[34]Savia Lobo, Google reveals an undisclosed bug that left 500K Google+ accounts vulnerable in early 2018; plans to sunset Google+ consumer version, available at <https://hub.packtpub.com/google-reveals-an-undisclosed-bug-that-left-500k-google-accounts-vulnerable/>(Accessed on Mar,28, 2021)
[35]Dan Swinhoe, the biggest data breach fines, penalties, and settlements so far, available at <https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html>(Accessed on Mar,28, 2021)
[36]Colin Lecher,Facebook app developers leaked millions of user records on cloud servers, available at<https://www.theverge.com/2019/4/3/18293978/facebook-app-developers-leak-user-records-data-cloud-servers>(Accessed on Mar,28, 2021)

Gal, CTO of Israeli cybercrime intelligence firm Hudson Rock, Troy Hunt of haveibeenpwned.com, and others, had confirmed the breach.[37]

THE PERSONAL DATA PROTECTION BILL

India is the latest country to announce plans to enact data privacy legislation. The proposed Personal Data Protection Bill (PDPB) aims to completely revamp India's present data protection rules. The Bill is largely based on the proposed draft of the Personal Data Protection Bill, 2018 ("Draft Bill"), which was attached to the report provided to the Government by the Committee of Experts chaired by Justice Srikrishna (Retd.)

The primary constituents of the Personal Data Protection Bill:

The proposed bill defines **Data** as "any information, opinion, facts, concepts, and it can be categorized as health data, biometric data, genetic data, financial data etc."

Personal Data is the "data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information".

This bill also focuses on specific sorts of data known as sensitive personal data, which necessitates increased protection and safeguards. It covers health information, financial information, sex life, sexual orientation, biometric information, genetic information, caste or tribe, political or religious belief or affiliation, and so on. Another type of data is essential personal data, which requires a greater level of protection and will only be processed in India. The data in this category is not yet specified, but the Central Government of India will notify the entire list in the future. The following entities are involved: The owner of the data is referred to as the Data principal. A data fiduciary is described as "any person, including the state, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of the processing of personal data". Data processor, who might be a data fiduciary or a third party who processes data on the data fiduciary's behalf. This bill expressly specifies that the job of data fiduciary is to protect the data of an individual. Other

[37]Abi Tyas Tunggal, the 52 Biggest Data Breaches, available at www.upguard.com/blog/biggest-data-breaches (Accessed on Mar,28, 2021)

institutions that may be engaged include independent auditors who do data audits, the Data Protection Authority of India (DPAI), which establishes rules and makes legal judgments based on information from the data principal, data fiduciary, and independent auditors.

The Joint Parliamentary Committee (the "JPC") delivered its report on India's proposed Data Protection Bill (the "Bill") on December 16, 2021.

The JPC suggested in its report a staged approach to implementing the legislation, beginning with the appointment of different government offices, such as the Data Protection Authority ("DPA"), and completing full implementation of the law within 24 months. A draft version of the Bill was also included in the JPC's report.

Following are the key recommendations made by the Committee with regard to privacy of an individual:

1. Data for economic growth and regulation of non-personal data: The Report emphasises on the economic significance of data, naming it an "asset of national importance." [Para 1.2.10, Report.] and stresses on the need to 'unify data sets' [Para 1.2.7, Report.] to fuel innovation. In keeping with this concept, the Committee proposes broadening the scope of the law to encompass non-personal data. [Para 1.15.8, Report.] Notably, it advises that the Bill include a separate rule for non-personal data. This is a shift from prior iterations, which were limited to personal data protection, and significantly undermines the original bill's privacy-focused orientation.

2. *Data localisation*: The Committee believes that keeping data on Indian territory is critical for national security, privacy, economic, geopolitical, and innovative reasons. [Para 1.9.4, Report.] As a result, it recommends that the government bring back mirror copies of any sensitive and vital personal data that has already been kept abroad. It proposes that all businesses operating in India should 'gradually' localise their data. [Para 1.15.17.5, Report] The Committee urges the government to develop a comprehensive data localisation policy that addresses issues such as developing adequate infrastructure for such local storage, assisting startups in meeting localisation requirements, and keeping the government's 'ease of doing business' objectives in mind. [Para 1.15.17.6, Report]

3. *Testing of hardware and software products*: Considering the privacy issues of data

collecting by hardware devices, the Committee recommends that the government institute a certification mechanism for all digital and IoT devices, and that testing centres be established throughout India to provide such certifications. These facilities/laboratories should also be able to test an individual's device and determine whether or not it fulfils data security requirements, failing which they should alert the Data Protection Authority (DPA) and take action against the manufacturer. [Para 1.15.16.3, Report.]

4. ***Data breaches***: The JPC suggests that the DPA develop laws and regulations governing data breaches based on a set of guiding principles. These include safeguarding the privacy of the data principal while reporting breaches, forcing enterprises to justify reasons for disclosing the breach late, and requiring companies to keep a log of data breaches for periodic review by the DPA. [Paragraph 1.15.10.2, Report.]

5. ***Social media***: According to the Committee, social media sites should be held more accountable. It refers to numerous social media phoney identities and bots that propagate fake news and perform destructive activities. It suggests account authentication via ID verification for each user. It also feels that the intermediary structure established by the Information Technology Act of 2000 (IT Act) has failed, and hence advises that these businesses be recognised as "publishers" in certain instances, particularly when dealing with harmful information from unverified accounts. It also proposes that all international social media businesses establish an Indian office or face being restricted from providing services in India. [Para 1.15.12, Report.]

6. ***Indigenous alternative to SWIFT****:* The JPC suggests that an alternate payment system to the 'SWIFT' system be established in India. According to the JPC, this will improve financial data security and strengthen the home economy.

7. ***Scope of the Bill extended to include non-personal data***: The 2019 Bill only addressed the protection of "personal data." The JPC, on the other hand, suggests calling the Bill the 'Data Protection Act' — a single legislation that will govern both personal and non-personal data (NPD), including anonymized data. It maintains mandated NPD sharing with the government., [Para 2.271, Report.] and suggests that the data regulator be given authority to probe NPD data breaches. Stakeholders have previously expressed concerns about including NPD within the personal data protection law, arguing that the goal of a personal data regulation

is to protect personal information. In contrast, the goal of NPD regulation is to generate value from data, and regulating both under one legislation will dilute such goals.

8. ***Processing personal data for reasonable purposes***: The PDP Bill permits businesses to process data for non-consent-based justifiable uses. The DPA will specify appropriate objectives while considering certain circumstances, including the interest of a data fiduciary. The JPC now suggests inserting the word 'legitimate' before 'interest' to the list of criteria the DPA should examine when evaluating such objectives. While this appears to be a primarily aesthetic modification, it may require corporations to demonstrate that their interest in each processing activity is justified.

9. ***Transparency of algorithms and processing methods***: To improve transparency and prevent misuse, the JPC proposes that data fiduciaries give facts about the fairness of algorithms and data processing processes.

10. ***Processing children's data***: The Report finds that the idea of a "guardian" as a distinct type of data fiduciary is unrealistic and may weaken the goal of protecting children. As a result, the Committee proposes that this idea be removed entirely. It also suggests that all data fiduciaries be prohibited from conducting profiling, tracking, or behavioural monitoring of children, as well as targeted advertising intended at children, and from processing personal data that may cause serious harm to children. Previously, this bar only applied to guardian data fiduciaries.

11. ***Reporting of data breaches***: The Committee advises that businesses report data breaches to the DPA within 72 hours. [Paragraph 2.111 of the JPC report.] It also proposes that companies notify data breaches in all instances, rather than just when the breach may cause harm to the data subject, as was the provision in the 2019 Bill. Furthermore, the JPC proposes that the Bill cover breaches of non-personal data as well. [Para 2.107, Report.]

12. ***Data protection officer***: The Committee recommends that substantial data fiduciaries employ a Data Protection Officer (DPO), who will play an important role in corporate management. The DPO should be a senior officer or top executive employee with the technological expertise of the appropriate essential data fiduciary's activities. [Paragraph 2.136, 2.137 and 2.138 of the JPC report.]

13. ***Cross-border data transfers***: The Committee recognizes the risks connected with cross-

border data flow must be aligned with development. [Paragraph 1.9.4 of the JPC report.] The JPC advises introducing another authorization layer for transmitting sensitive personal data (SPD) (SPD). Before sanctioning a transfer of SPD under a contract or intra-group plan, the DPA will need to confer with the federal government again. [Paragraph 2.149 of the JPC report.] According to the Committee, these intra-group programs should be approved only if they are aligned with 'public policy' or 'State policy'. [Paragraph 2.150 of the JPC report.] The Committee also suggests including a provision requiring that no private data be disclosed with any foreign government and agency without the approval of the central government. [Paragraph 2.154 of the JPC report.] Laws requiring central government clearance for contract-based cross-border flows may impose further bureaucratic impediments to data movement — which, as the Committee observes, is crucial to digital economy growth. [Para 1.9.2, Report.]

14. ***Certification of hardware and software products****:* The JPC also views abuse of digital devices and hardware as a serious problem that necessitates the engagement of the DPA. It suggests that the DPA develop a framework for monitoring, testing, and certifying hardware and software for computing devices in order to ensure "data integrity". [Para 2.201, Report.].

15. ***Penalties:*** The JPC advises that the central government be given the authority to impose fines through rules. Although, it keeps the restrictions that would limit the amount due to Rs. 15 Crores or 2-4 percent of corporations' worldwide sales. [Rec. No. 71]

16. ***Offences by companies****:* The Committee holds accountable the employees of an offending corporation that are in authority of 'that section of the company to which the infringement pertains.' Previously, the bill specified that the person in general command of the organisation should be held liable. [Para 2.256, Report.][38]

CONCLUSION/SUGGESTION

In today's world, governance is hard to achieve without the successful introduction of digital services and the active participation of citizens. Many factors, including unauthorized use of personal data, may jeopardize privacy on social networking sites. So, access to users' personal data should be restricted. Authorities should respect the right to privacy by restricting how private entities, not only intelligence services and the police- handle personal data. Courts have also recognized that collecting, using, storing, and exchanging private information can violate

[38] Report of the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill, 2019

one's right to privacy. The statutes that were recently introduced in the regulations are incomplete, but they are not deficient. They need precision and substantiation rather than outright rejection. Mandating ex-ante ex-parte court orders would be the better option, given the legal approach to data collection. Since everybody is hooked up to the internet, and our private information can be exchanged with others on websites like Google Facebook, Twitter, Snapchat, and a variety of other sites, due to which there is a clear need for appropriate and strict privacy laws. In the twenty-first century, information may be a powerful source of money. Before posting your post or pictures, think of who would be able to read, react to, or comment on them. An individual must consider if you want your social media messages and photos to be visible to everyone, only friends, or friends of friends while changing the privacy settings for each site. All of this shows that in this social media era, there is a dire need for effective laws on digital privacy. However, it's necessary to keep in mind that some challenges still exist, and those new challenges are being added to the challenges that already exist. Governments, some intelligence departments, private corporations, and other unidentified organizations are all constantly scrutinizing the digital world. As a result, the problem of personal privacy, protection, and digital security must be properly addressed.