Page 5086 - 5101 **DOI:** *https://doij.org/10.10000/IJLMH.111101*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

Concerns with Privacy: An Indian Context

VARUNI TEWARY[1] AND ARUSHI SHARMA[2]

ABSTRACT

The management of personal data in the digital world raises concerns regarding privacy and security of information. Privacy can be defined as access of an individual, group, or organisation to information. Data privacy is one of the most critical challenges faced by the contemporary modern society. While it is an assumption that privacy can solve the problems we face in the digital world, however, in reality, privacy comes with its own set of issues. The primary aim of this paper is to qualitatively analyse the concerns around privacy. This research explains how data protection laws can be difficult to implement and can be a threat to privacy itself. The paper explores the intersections between privacy and social order and examines how production, control, and management of privacy are unequally distributed. As global negotiations today revolve around the transfer and security of data, the Indian Government has proposed the Personal Data Protection (PDP) Bill, 2019. This paper aims to unravel these issues and look at the approach of the Indian parliament in solving them through the PDP Bill.

Keywords: *Privacy, Jurisdiction, Social Control, Inequality, Surveillance.*

I. INTRODUCTION

The world is moving towards a digital society. The internet has opened various channels of communication and has allowed the world to lose its borders. The digital economy is driven by the collection and analysis of ubiquitous amounts of data on the internet. This data is reflective of all the internet users and is of immense value. The platforms use this data to facilitate economic transactions and to improve interaction in the virtual world. The government uses this data for better policy planning and ensuring state security. The digital world is growing fast, and it is estimated that by 2022 global Internet Protocol (IP) traffic is projected to reach 150,700 GB per second.[3]

As the world remains in the early stages of this digital society, various stakeholders of the society are raising issues and questions regarding the data generated on the internet. It is believed that the massive data collection that takes place on the internet is a disadvantage to its

[1] Author is a student at Gujarat National Law University, Gandhinagar, India.
[2] Author is a student at Sri Venkateswara College, University of Delhi, India.
[3] United Nations Conference on Trade and Development, *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries* (2019).

 [ISSN 2581-5369]

users as they are deprived of their privacy. Data privacy refers to the processing, access, and storage of users' data. There are two kinds of data broadly, public data and personal data. The former type includes information that is accessible to the public at large. The latter type is the information that is not available in the public domain and is likely to reveal an individual's behaviour and preferences. In most cases, it is the breach of private data that people are concerned about when referring to data privacy. As the number of users increases on the internet, governments and active citizens are pushing to create laws that can monitor the internet and ensure accountability in cases of privacy breach.

There are a lot of legal, moral, ethical and social concerns related to privacy. These concerns, however, are not mutually exclusive and remain entwined. One issue related to privacy is that of the jurisdiction of the data laws. The problem of jurisdiction arises from the fact that the internet is transnational. This means that communication and transactions that happen on the internet can cross territorial boundaries. In such situations, it becomes difficult to determine the laws which are applicable in case of a privacy breach. As the available literature on the matter indicates, the countries remain divided on the issue of jurisdiction, and this leads to extraterritorial laws being enacted in various parts of the world.

The second issue is that of government surveillance. It is contended that the right to privacy should be available to individuals against private parties as well as the government. A contrary argument is that the excessive use of right to privacy can undermine the State's welfare role in our digital society. Most governments admit to surveillance, but they defend it in the name of security of the State and its citizens. The existing research on the topic indicates that there seem to be no concrete solutions here, and the governments need to be held accountable by their citizens.

Privacy is also affected by the social order. The paradigms of disclosure and concealment of personal information affect social relationships. This means that changes in the social order of a society can have implications for privacy. Before industrialisation, society was more community oriented than individualistic. It was in the industrialisation era that society became individualised and came to respect the idea of privacy. As the industrialised society again changes into a digitised one, privacy will be affected and will affect people's lives accordingly.

Another issue with privacy is that of inequality. It is a common misconception that privacy is a right and that every individual has equal access to it. However, in reality, privacy is a resource

 [ISSN 2581-5369]

with limited access,[4] and hence it creates social divisions. The relative ability of social actors to manage privacy and its effects is unevenly distributed. As the digital economy and society are on the rise, the accessibility to privacy becomes the basis of inequality.

Countries across the globe have tried to tackle privacy issues, including India. Recently, the Government of India introduced The Personal Data Protection Bill, 2019, on December 11, 2019. [5] The bill trifurcates data into three categories – personal data, sensitive personal data and critical personal data.[6] The PDP Bill is supposed to be a right based and a consent based law. The bill resembles other data laws present in various countries in those areas of transfer of data and penalties but yet differs in certain key provisions. The bill, if enacted, will be the first comprehensive data privacy law in the country. Presently, it has not been passed by either house of the parliament and has been referred to the standing committee, which is yet to give its report on the bill. The ramifications of the PDP Bill will be known only when it comes into force.

The present article focuses on the issues with privacy in an analytical manner. It explores how these issues affect privacy and people at large in the society. The aim of this paper is to unravel the issues with data protection and look at the approach of the Indian parliament to solve these issues through the PDP Bill. For the purposes of this article, the terms data protection and privacy have been used interchangeably. However, in reality, protection is a broader concept when compared to privacy. The recommendations and findings of this paper can be of great interest to policymakers in the area of data protection.

II. JURISDICTION

The internet is an architecture that has revolutionised the way this world communicates. It has opened various channels of data sharing and access for the people. In the past cross border interactions were rare exceptions. Today with most of our activities shifting online, there is an increased possibility of conflicting laws coming in contact as multiple jurisdictions are invoked while working on the internet. It has become increasingly challenging to determine the applicable laws and enforce the redressal mechanisms. This situation is a concern for all stakeholders, including governments, digital platforms, civil society groups and the individual users of the internet.

[4] D. Anthony, C. Campos-Castillo & C. Horne, *Toward a sociology of privacy*, 43 ANNU. REV. SOCIOL. 249, (2017). [hereinafter Anthony].
[5] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, Dec. 11 2019 (India). [hereinafter Bill].
[6] Radhika Iyer, Lakshmi Pradeep & Anshul Chopra, *India: The Personal Data Protection Bill, 2019*, MONDAQ (Jan. 07, 2020), https://www.mondaq.com/india/data-protection/880766/the-personal-data-protection-bill-2019.

 [ISSN 2581-5369]

One legal issue that arises from the internet revolution is that of data protection and storage. Data protection is the right of an individual in how the data identifying them or pertaining to them is processed. This processing is defined under a set of laws. Like the internet itself, data storage and processing on the internet is also transnational. This means that if an Indian user gives his data to a social media platform like Facebook, then his data is not stored locally in India but is stored with the company in the US. In such a situation, the question arises that when there is a breach of data, then is the company liable under US data protection laws or Indian data laws or if they are liable at all. Although the principles of data protection remain the same across countries, the details of these laws differ substantially.[7]

There are various reasons because of which jurisdictional issues arise within data privacy laws. The first reason is that data privacy cannot be classified as either a part of public law or private law.[8] Allowing it to be fully under public law would mean applying only domestic laws in cases of dispute. However, data protection falls at the intersection of public and private law and therefore cannot be put in a watertight compartment. Data protection laws have various sources – human rights, consumer protection, to name a few and hence it is challenging to have a single jurisdiction. Another reason which remains core to the jurisdiction issue is the difference between the common and civil law systems.[9] There is a history of extraterritorial application of laws in the common law system. This means that a common law court can order a company located in another territory to comply with the laws of the country where a case is lodged. A classic case for extraterritorial jurisdiction is the Microsoft Search Warrant case.[10] A US district court in the present case ordered the company Microsoft to fetch data from its Irish subsidiary and comply with the Stored Communications Act. In appeal, the Second Circuit had different views and held that the lawmakers did not intent to make the law with extraterritorial jurisdiction.[11] Later on, the Congress explicitly mentioned the extraterritorial nature of the act and the court's decision was vacated.[12] This order from the district court demonstrates the irregularities when it comes to data protection laws and their interpretations.

Various legal systems have tried to make laws that can reduce the complexities involved with data protection. One such endeavour is the General Data Protection Regulation (GDPR) of the

[7] Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 1),* 18 INT. J. LAW INF. TECHNOL. 176, (2010). [hereinafter Kuner].
[8] *Id.*
[9] P. Sean Morris, *"War Crimes" Against Privacy – The Jurisdiction of Data and International Law*, 17 J. HIGH TECH. LAW. 1, (2016).
[10] Microsoft Corp. v. United States, 138 S. Ct. 1186 (2018).
[11] Microsoft Corp. v. United States, 130 HARV. L. REV. 769, (2016).
[12] Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C §§ 2701–2712 (2016).

European Union (EU). This law applies to organisations even outside the EU but under specific circumstances like when the processing activities are related to (a) the offering of goods or services; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.[13]Personal data has been clearly defined under the act and the controller of the information is further banned from processing this data with a few exceptions that is of explicit consent and necessity of processing. The GDPR recognises the need for transfer and storage of data because of data's transnational nature. The transfer and receiving, however, is only limited to jurisdictions that the European Commission deems to be with adequate data protection.[14] The GDPR model appears to be preferred in numerous countries that have recently adopted data protection legislation. A variation of this law, which may be described as a co-regulatory model, was earlier adopted in Australia in the form of the Privacy Act and Canada in the Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA).[15] On the other hand, is the US has multiple laws which act as data protection laws. Some of these have extraterritorial jurisdiction, like the Children's Online Privacy Protection Act (COPPA) which applies to any website which collects information from minors living in the US.[16] Other acts like FTC,[17] HIPAA,[18] FERPA,[19] etc., deal with industry-specific data protection. Therefore, unlike the EU, the US does not have one single data protection law.

In the case of India, the Supreme Court recognised the right to privacy as a part of Article 21 of the constitution in case of Justice K.S Puttaswamy (Retd.) v. Union of India and Ors.[20] The legislative framework in India is like the US which means that India still lacks comprehensive legislation on the data protection. This started to change in December 2017 as the Indian government appointed the data protection committee chaired by Justice Srikrishna. This committee did an in-depth analysis and sought comments from all stakeholders, and their report became the foundation for the Personal Data Protection Bill, 2019. This bill is also extraterritorial when it comes to processing of data outside India and allows processing only if it is (a) in connection with any business carried on in India / systematic offering of goods or services; or (b) in connection with any activity which involves profiling of Data Principals within the territory of India.[21] In most aspects, the PDP Bill resembles the GDPR. However,

[13] Commission Regulation 2016/679, art. 3, 2016 O.J. (L119).
[14] See *id.* at art. 45.
[15] *White Paper of The Committee of Experts on A Data Protection Framework for India,* GOVERNMENT OF INDIA, https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf.
[16] Kuner, *supra* note 7.
[17] Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2006).
[18] Health Insurance and Portability Act, Pub. L. No. 104-191, 1996 (110 STAT.) 1936 (1996).
[19] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1974).
[20] Justice K.S. Puttaswamy and Ors. v. Union of India (UOI) and Ors., AIR 2017 SC 4161.
[21] Bill, *supra* note 5, § 2.

 [ISSN 2581-5369]

unlike the latter, which allows the processing of personal data when necessary, the PDP Bill does not allow the processing of critical personal data out of necessity. The bill allows for the transfer of sensitive personal data with some restrictions outside India. These transfers are permitted only if (a) certain provisions are included which are pre-approved by the data protection authority, or (b) the government approves the location or organisation for the transfer, or (c) the data protection authority specifically approves such a transfer as necessary for any specific purpose. Further, such transfers must be consented to.[22] Therefore the bill, when enacted, will have far-reaching consequences on platforms doing business in India because of its extraterritorial nature.

III. SURVEILLANCE

Surveillance refers to any collection and processing of personal data, whether identifiable or not, for purposes of influencing or managing those whose data have been garnered.[23] Transactions done on the internet, in particular, generate detailed electronic prints that expose an individuals' preferences, interests, and behaviour. Thus, the internet provides an unprecedented means to observe the user's internet activity unobtrusively and to collect copious amounts of data about individuals and their transactions which is used by both the private as well as public players. The companies use this data for consumer profiling, while the governments use it for profiling their citizens. In the latter case, the government uses the internet as a tool to collect data to monitor citizen behaviour and prevent crimes.[24] In some commercial instances, the individual is aware that the information that they are producing is being collected, but in most instances, the individual is not informed about their data being collected and processed. In some cases, this data is made accessible to third parties for different purposes of which the users are unaware. For example, law enforcement agencies routinely check social media sites for information that might be useful in an investigation.

For the longest time, governments have defended their actions in the name of national security. Since the increase in cybercrimes which includes virus attacks, network break-ins, online scams etc., cybercrimes have become the third highest priority, after counter-terrorism and counter-intelligence. The nature and seriousness of the security threats would seem to make surveillance a welcome and justifiable practice. At the same time, given the possibility of increased cyber-attacks, fraud, and further terrorist activity, the rapid evolution of the

[22] Bill, *supra* note 5, § 34.
[23] DAVID LYON, SURVEILLANCE SOCIETY: MONITORING EVERYDAY LIFE (McGraw-Hill Education, 2001).
[24] Karina Rider, *The privacy paradox: how market privacy facilitates government surveillance*, 21 INF. COMMUN. SOC. 1369, (2017).

 [ISSN 2581-5369]

government initiatives to enhance surveillance has forced a debate about consolidating security and privacy along with the debate around security as an impediment to privacy. Many countries indulge in data collection for security reasons. In the United Kingdom, the minister of the Crown has to issue a certificate of surveillance for monitoring of an individual for national security reasons. Although the legislation exempts personal data from this surveillance, the scope of this exemption remains ambiguous.[25] In Canada, organizations are to disclose personal information of users without their knowledge in cases of national security and international affairs.

This surveillance is not limited to criminal investigations. The recent COVID-19 pandemic has illustrated the need for government surveillance. Sensitive health information in the form of contact tracing, large-scale testing and the maintenance of public health records (symptoms and quarantine regulation) has to be collected not just for citizens but also for non-citizens across the country.[26] The access to the internet and advanced methods of information technology provides an unprecedented capacity to collect and disseminate information. Internet technology has become integral to public health surveillance as it allows to track an outbreak in real-time and facilitates public health responses to outbreaks and emerging diseases.[27]

The proposed Personal Data Protection Bill follows the footsteps of the other data privacy laws and exempts the government agencies from gathering personal data of the citizens. According to the draft, the government could exempt its data fiduciaries from rules that govern the processing of personal data on the grounds of national security, public order, and friendly relations with foreign states. [28] However, this will be subject to procedures, safeguards, and oversight mechanisms of the respective agency. The bill also mandates organizations to give the government any non-personal data when demanded. Non-personal data refers to anonymized data, such as traffic patterns or demographic data.[29] Therefore, the PDP Bill is driven by the underlying objective to protect data relating to individuals. However, the proposed law sets accountability only for private players and remains vague on the remedies available against the State. Civil society groups have criticized the bill as it openly allows

[25] Stephen A. Oxman, *Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?*, 24 B.C. INT'L & COMP. L. REV. 19, (2000).
[26] Aditi Subramaniam & Sanuj Das, *The Privacy, Data Protection and Cybersecurity Law Review: India,* THE LAW REVIEWS (Oct. 21, 2020), https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/india.
[27] John S. Brownstein, Clark C. Freifeld, & Lawrence C. Madoff, *Digital disease detection--harnessing the Web for public health surveillance*, 360 N. ENGL. J. MED. 2153, (2009).
[28] Bill, *supra* note 5, § 35.
[29] Bill, *supra* note 5, § 91(2).

government surveillance.[30]

Apart from this, the PDP Bill states that one copy of all and sensitive personal data needs to be stored in India, and certain data classified by the draft as 'critical personal data' needs to be stored in India only and cannot be transferred outside India.[31] It is argued that this provision would allow investigative agencies to access data easily for law enforcement. This localization is also thought to push for data sovereignty when under foreign cyber attacks. However, it is felt that this move would only make the data more vulnerable to government monitoring. Therefore, it is evident that the bill does little to allay the fears of surveillance.

IV. SOCIAL ORDER

During the 20th century, an essential topic of discussion was the role of privacy in social relationships and order, and privacy was seen as a component of a well-functioning society.[32] Social order refers to the extent to which members of a social group cooperate to achieve collective ends.[33] Privacy and social order overlap as access to information and visibility is thought to be critical to social control.[34]

Individuals have always collected, analysed, recorded and disseminated information about. People watch each other, they gossip, and they react to the behaviours they observe.[35] With the development in information and communication technology (ICT), new dimensions of monitoring and surveillance are used by institutions and governments. With changing methods and levels of surveillance and the shifts in the social structure, the perception towards monitoring and privacy has changed over time and place. For example, in primitive societies where face to face interpersonal interaction is dominant, and people work in close proximity, the individual behaviour is publicly visible, due to which secrecy becomes difficult to obtain.[36] With the rise of industrialisation and the great transformation, living patterns in societies became more individualistic, and privacy became a critical aspect. Privacy plays an essential role in maintaining social relationships, and an individual's control over his personal information dictates the category of relationship with other individuals. Privacy affects not only one-on-one interpersonal relationships but also groups and communities more broadly. It has

[30] Karishma Mehrotra, *Explained: The issues, debate around Data Protection Bill,* IE (Dec. 7, 2019, 8:31 AM), https://indianexpress.com/article/explained/personal-data-protection-bill-cyber-security-hacking-6153015/.
[31] Bill, *supra* note 5, § 40.
[32] P.M. Regan, *Response to privacy as a public good,* DUKE LJ ONLINE 51, (2015).
[33] M. HECHTER & C. HORNE, THEORIES OF SOCIAL ORDER: A READER (Stanford University Press, 2003).
[34] M. HECHTER, PRINCIPLES OF GROUP SOLIDARITY (University of California Press, 1988).
[35] M. Feinberg, R. Willer & M. Schultz, *Gossip and ostracism promote cooperation in groups,* 25 PSYCHOL. SCI. 656, (2014).
[36] R.A. Posner, *A theory of primitive society, with special reference to law,* 23 J.L. & ECON. 1, (1980).

 [ISSN 2581-5369]

implications for group boundaries, cohesion, and collective action. Patterns of disclosure strengthen ties among group members and create stronger boundaries between the group and outsiders.[37]

Any intrusion upon an individual's privacy would mean that he feels unable to be immersed in the social interaction and share its meaning.[38] A person who deliberately gains access to information that the other person wants to keep secret violates the other person's space only through information control.[39] People tend to decide their level of disclosure and concealment depending on the type of social relationship with the other party. For example, the level of disclosure expected from a life partner is not similar to that of a professional colleague. This distinction becomes more critical with the increasing anonymity in the highly industrialised urban setting. Therefore, when people lose control over their personal information and their ability to disclose or conceal data, any threat to privacy is met with resistance.

Privacy provides an opportunity for people and organisations to discuss matters in the space of personal choice and free of unreasonable police interference.[40] Privacy is the basis for the development of individuality as it protects personal autonomy.[41] It becomes necessary and critical to support functioning, stable interpersonal relationships to maintain the social order.

However, Governing bodies have always tried to ensure compliance and control by collecting information. Monitoring and visibility become essential to social control as violations can only be punished if others know the violation occurred.[42] Observability provides transparency of social arrangements and makes modelling of behaviour possible.[43] In addition, the mere awareness of being monitored controls the individual behaviour, irrespective of the presence of a monitoring body.[44] Governments have justified monitoring to ensure everyday safety and capture of bad actors - as people are more accepting of monitoring that appears to target the other, that is, members of an outgroup rather than themselves. For example, citizens may be willing to accept a check on internet activity when they believe it targets criminals and anti-social elements. People may disagree when they believe the surveillance targets them, such as when teenagers talk in code when they know the adults are monitoring their conversation.

---

[37] Anthony, *supra* note 4.
[38] M. Becker, *Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy,* 21 ETHICS INF. TECHNOL. 307, (2019). [hereinafter Becker].
[39] Becker, *supra* note 38.
[40] A.F. Westin, *Privacy and freedom,* 25 WASH. & LEE L. REV. 166, (1968).
[41] S.T. Margulis, *Privacy as a social issue and behavioral concept,* 59 J. SOC. ISSUES 243, (2003).
[42] M. Hechter, *Nationalism as group solidarity,* 10 ETHN. RACIAL STUD. 415, (1987).
[43] R.L. Coser, *Insulation from observability and types of social conformity,* AM. SOCIOL. REV. 28, (1961). [hereinafter Coser].
[44] Becker, *supra* note 38.

High levels of monitoring, which violate privacy norms, often lead to resistance, disrupting the existing order. Monitoring produces resentment as it conveys a lack of trust and suspicion by the governing bodies. Any invasion of privacy disturbs control over and access to an individual's personal sphere. This notion of privacy is closely related to secrecy. With the digital age being characterised by the omnipresence of surveillance and monitoring, the levels of observation and the corresponding consequences have changed the ideas about privacy.[45] The concern is often about the constant observation resulting in the loss of autonomy over one's personal space. The commercialisation of privacy invasion affects individuals' decision-making, where they do not function as independent thinkers. This becomes a more significant threat to social order as peoples' interaction and reaction is influenced by the invisible algorithms used to seduce users.

Additionally, information about others' deviance may paradoxically increase the likelihood of future deviant behaviour.[46] Evidence suggests, for example, that visible deviance is contagious,[47] and undermines existing rules,[48] whereas ignorance of violations maintains norms,[49] which will altogether pose a threat to a well-functioning society.

On the one hand, monitoring may increase control and compliance, which is a key to social control.[50] It may also produce unintended consequences such as normalisation of deviance and compromising people's trust in the social order. Privacy has implications for people's relationship with each other, community, and social institutions. In general, the reaction of people on the issues of privacy and monitoring is mainly dependent on the use and level of surveillance by the governing bodies and their perception of it. Finding the optimal balance between disclosure and concealment of personal information is vital for social order.

The Personal Data Protection Bill, 2019, primarily focuses on the people of India and protecting their privacy. It seeks to provide more control to Indians over their personal information and create a culture towards respecting the informational privacy of individuals.[51] As the bill provides a separate legal ground for organisations to process employee personal

[45] *Id.*
[46] Anthony, *supra* note 4.
[47] A. Diekmann, W. Przepiorka, & H. Rauhut, *Lifting the veil of ignorance: An experiment on the contagiousness of norm violations*, 27 RATION. SOC. 309, (2015).
[48] K. Keizer, K., S. Lindenberg, S. & Steg, L., T*he spreading of disorder*, 322 SCIENCE 1681, (2008).
[49] J.A. Kitts, *Collective action, rival incentives, and the emergence of antisocial norms*, 71 AM. SOCIOL. REV. 235, (2006).
[50] R.B. Cialdini, *Descriptive social norms as underappreciated sources of social control*, 72 PSYCHOMETRIKA 263, (2007).
[51] Dhrtimaan Shukla, Sonali Saraswat & Harbani Gill, *Personal Data Protection Bill, 2019: What Indian citizens can expect*, PwC (Jun. 10, 2021, 01:05 PM), https://www.pwc.in/assets/pdfs/consulting/cyber-security/data-privacy/personal-data-protection-bill-2019-what-indian-citizens-can-expect.pdf.

 [ISSN 2581-5369]

data necessary for employment purposes, it also allows employee-sensitive personal data to be processed only based on consent. Increased individual control over personal data will forge a relationship of trust and transparency. The bill further grants greater control and access to personal information giving people autonomy over their information fostering stable and well-functioning social relationships. However, as it asks for data storage in India for improved access over law enforcement, the bill compels the citizens to see it as a threat to their autonomy over the concealment and disclosure of data and, hence, is met with resistance.

V. SOCIAL INEQUALITY

Privacy is "a scarce social commodity ...[whose] possession reflects and clarifies status divisions" (prestige or esteem accorded by society) and power differences (the ability to acquire resources despite others' resistance).[52] Thus, the distribution of privacy reflects inequality. In addition to being unequally distributed, the production and management of privacy may also create inequality among social actors. It is important to note that this creates a vicious cycle where the distribution of control over personal space is unequally distributed due to the existing divide, leading to the penetration of more profound inequalities.

Because socio-economic and moral status and power shape who has privacy, privacy is unequally distributed;[53] and because privacy management requires skills and resources, actors vary in their ability to limit access to themselves and gain access to others.[54] Accessibility and visibility are distributed in an unequal way within the social structure. The lower status actors have a lesser ability to manage 'breaches' than the higher-status actors. In some part, this is because their social circumstances make them more vulnerable. For example, sick people have more sensitive data and hence have more vulnerability than healthier people; children have less privacy than adults; people living in common community homes such as urban slums have less privacy than people living in gated communities. Further, the economically weaker sections must forgo their privacy and give more personal data to be beneficiaries of the government programs. "[I]nsulation from observability, and access to it, are just as important structural elements in a bureaucracy as the distribution and delimitation of authority."[55]

"[T]he allocation of privacy ...is a clear measure of one's status and power in any given situation."[56] It is easier to invade the privacy of weaker sections of society. For example – in

[52] B. Schwartz, *The social psychology of privacy*, 73 AM. J. SOCIOL. 744, (1968).
[53] C. Warren & B. Laslett, *Privacy and secrecy: A conceptual comparison*, 33 J. SOC. ISSUES 43, (1977).
[54] Anthony, *supra* note 4.
[55] Coser, *supra* note 43.
[56] C.E. NIPPERT-ENG, ISLANDS OF PRIVACY 164 (University of Chicago Press, 2010).

Indian society, women do not enjoy as much privacy in the domestic domain as men do. Often because women do not have access to personal devices or do not know how to operate those, they are compelled to share sensitive information to get help with technical difficulties. The findings of a study reveal significant differences in the behavioural models and identify pivotal factors that shape the use of Information and Communication Technology by members of different socio-economic groups.[57] Not only is privacy unequally distributed across social groups and social conditions, but the consequences of the differential ability to gather and use private information may, in turn, affect inequality.[58]

The social sorting as done by the so-called Big Data companies assigns worth to human lives and has real-life effects on people's life chances. Statistical discrimination occurs when decision-makers rely on objectively accurate correlations between group characteristics and outcomes and apply the correlation to all the individuals within the group category.[59] These classifications have remnants of the traditional biases in the society, be it based on class, religion, gender, race, socio-economic background.

The enhanced information regarding a large population can lead to the identification and creation of new hierarchies. Evidence suggests that even when equally monitored, the governing bodies suspect more of the people matching the 'typical' profile of the criminal—for example – focusing on young minority men or people from the so-called shady part of the town. Another way of discrimination caused due to privacy invasion is showing 'personalised' offers and advertisements where online advertisers target potential buyers based on their behaviour, income, or location. For example - The Orwellian potential of the new digital possibilities of social control can currently be observed in China. The Chinese authorities are experimenting with a "social score" that integrates various databases in order to evaluate the behaviour of companies, persons, and organisations. The score ultimately decides upon access to goods and services.[60] A hierarchy that becomes more conspicuous is the position of individuals as opposed to the internet giants such as Google, Amazon, and Facebook. The divide is based on the generation of huge amounts of data by observation of user interaction. While we are becoming increasingly transparent, the handling of data by corporations is becoming increasingly opaque. Trying to escape does not seem to be a viable option. [61]

[57] Hsieh, J. J. Po-An, Arun Rai & Mark Keil, *Understanding Digital Inequality: Comparing Continued Use Behavioral Models of the Socio-Economically Advantaged and Disadvantaged*, 32 MIS QUARTERLY 97, (2008).
[58] Anthony, *supra* note 4.
[59] *Id.*
[60] Marc Pirogan & Felix Beer, *Social order in the digital society*, DIGITAL SOCIETY BLOG (Jun. 10, 2021, 3:05 PM), https://www.hiig.de/en/social-order-in-the-digital-society/. [hereinafter Pirogan].
[61] Pirogan, *supra* note 60.

With the unprecedented increase in work from home, we see that the digital divide becomes more conspicuous as not everyone has equal access to the Internet. This divide overlaps with the 'spatial divide' as Internet density in rural areas is way lower than in urban areas and the 'gender divide' as far fewer women have access to smartphones than men.[62] With digitisation becoming the new norm, we must consider the large population excluded from this digital revolution. India's digital divide remains vast as more than 400 million people still have no access to the Internet.[63] India's digital divide is deep and persistent and has remnants of socio-economic divisions such as regional, economic and gender disparity. Increasing access to the digital world with limited knowledge of privacy norms creates more vulnerability. People from lower sections are less aware of the privacy norms and are indifferent towards monitoring and surveillance.

With the Data Protection Bill, 2019, the government contests that data localisation will increase the ability to tax Internet giants and help enforce data sovereignty. The bill does not protect individuals against the Indian government as effectively. It stipulates that "critical" or "sensitive" personal data, related to information such as religion, or to matters of national security, must be accessible to the government if needed to protect national interest.[64]

The critics of the bill contend that national security or reasonable purposes are open-ended terms, and it may lead to intrusion of the State in the private lives of the citizens which will undermine the fundamental right to privacy. It is essential to protect informational privacy as people with resources would manage the intrusions better and comprehensively than people from weaker sections of society. It is essential to note the technology giants like Facebook and Google criticises the protectionist policy on data protection as it suppresses the values of a globalised, competitive Internet marketplace.

Moreover, an individual must connect to achieve enhancement of social and cultural capital and achieve mass economic gains in productivity. Therefore, access is a necessary (but not sufficient) condition for overcoming the digital divide. Access to ICT meets significant challenges that stem from income restrictions.[65] The widespread digital divide also contributes to the inequality of access to goods and services available through technology. The Internet

[62] Ejaz Ghani & Saurabh Mishra, *Closing the digital divide*, FINANCIAL EXPRESS (Nov. 12, 2020, 7:15 AM) https://www.financialexpress.com/opinion/closing-the-digital-divide/2126724/.
[63] *Id.*
[64] Christophe Jaffrelot & Aditya Sharma, *Personal Data Protection Bill 2019 needs to be debated thoroughly*, IE (Jan. 07, 2021, 9:22 AM) https://indianexpress.com/article/opinion/columns/personal-data-protection-bill-2019-privacy-laws-7135832/.
[65] Karen Mossberger, Caroline J Tolbert & Michele Gilbert, *Race, Place, and Information Technology (IT)*, 41 URBAN AFF. REV. 583, (2006).

provides users with improved education and more skills, which can lead to higher wages.[66] Hence, the growth of the digital economy is essential to open a plethora of social and economic growth opportunities to allow people to overcome the existing inequalities, and any hindrance to this access will be a step towards the deepening of the existing digital divide.

VI. CONCLUSION

Due to recent innovations in information and communication technologies, the contemporary age is recognised with the omnipresence of devices, networks and data. It has made privacy an increasingly alarming topic for citizens, governments, business as well as academics. These technologies have enabled connections among all the stakeholders and facilitated the monitoring of individuals by multiple institutions and across multiple spaces. Throughout the day, information is collected, stored, aggregated, analysed, and disseminated. These new technologies have created an unprecedented set of privacy challenges.

Even with legal systems trying to make laws that can reduce the complexities and grey areas, there is much irregularity and ambiguity when it comes to data protection laws and their interpretation. The transnational nature of the Internet has increased the possibility of conflict due to multiple jurisdictions being involved and conflicting laws coming in contact. Due to internet's intersections with various other institutions, it is challenging to categorise its fine print. Even when data protection principles remain fundamentally the same in multiple countries, further details differ significantly. India lacked comprehensive legislation on data protection. Hence, the Indian government tried to define the data protection norms in India with the proposed Personal Data Protection Bill, 2019, by holding the data fiduciaries liable and protecting the data of Indian citizens. The bill trifurcated the data into three categories and mandated the storage within India's boundaries depending on the data type. The PDP Bill does not allow the processing of critical personal data out of necessity but enables the transfer of sensitive personal data with some restrictions outside India. The bill protects the citizens from third-party companies but remains unclear on the provisions of protection from State's intrusion.

With an unprecedented number of people joining the digital world every day, there is an increased means to observe the user’s internet activity and collect data as transactions done on the Internet generate detailed prints that tell us about the individual's preferences, interests and behaviour. This collection and processing of personal data is done by companies who use this for consumer profiling and governments to monitor their citizens. With increasing cybercrime,

[66] Ming-te Lu, *Digital divide in developing countries*, 4 J. GLOB. INF. TECHNOL. MANAG. 1, (2001).

 [ISSN 2581-5369]

surveillance is often justified for the consolidation of security. With better technologies, there is an unprecedented capacity to collect and disseminate information. Like other data protection laws, the proposed bill exempts government agencies from gathering personal data. On the one hand, it protects data sovereignty and sets accountability for private players, while on the other, the bill openly allows government surveillance and remains vague on the remedies available against State's intrusion.

Various researches highlight the ways in which privacy intersects with social structures in institutions to affect individuals, groups and communities. The researchers primarily focus on the effects of privacy threats on individuals and consequences of privacy for the functioning of society. Privacy's role in maintaining social order is complex, and the optimal balance is necessary for a well-functioning society. The government maintains compliance and control through monitoring and an individual's autonomy over personal space, when threatened, leads to backlash and becomes detrimental to the existing social order. An individual's access and control to his privacy are critical for inter-personal relationships and community – which is essential for social relationships. As an individual categorises relationships with concealment and disclosure of information, any threat to this control will threaten the social structure. The monitoring of actors leads to cooperation but often also leads to resistance and backlash.

Privacy is a resource unequally distributed in society, and the production, management of privacy and its effects further create inequality among social actors. These inequalities have particularly negative consequences for individuals and communities with low status and few resources. Apart from this, the digital divide in the developing world is persistent and profound. Weaker sections of society are more vulnerable than others mainly because of the differences already existing in the society, such as regional, gender, racial disparity.

With technology being incorporated into everything from cars, home management systems, wearable sensors, smartphones, and these databases being integrated across the domains of education, justice, healthcare, public transportation, government and countries, there is an increase in information and an associated loss of privacy. The laws need to have coherent transnational regulations and norms when it comes to data privacy. Any conflict in jurisdiction or laws have to addressed concerning citizen's fear and making laws more specific and less ambiguous. Apart from this, the effects of regulations like the Personal Data Protection Bill, 2019, can be estimated after these are enacted as laws.

There is a need to evaluate and understand the individual and collective goods in relation to privacy changes. Future work is needed to examine the secondary effects that are the

 [ISSN 2581-5369]

consequences of changes in privacy for society's functioning and organisation and how the spread and use of information and communication technology affect trust in social institutions. We need to further examine the role of privacy in maintaining, increasing, or flattening the status hierarchies and exploring how the spread and use of ICT create new status hierarchies.

*****

 [ISSN 2581-5369]