Lakshya Sharma & Siddharth Panda, 'Into the Orwellian Dystopia: A Comparative Analysis of Personal Data Protection Bill 2019 vis-à-vis Indian Privacy Jurisprudence' (2021) 7(2) NLUJ L Rev 1

# INTO THE ORWELLIAN DYSTOPIA: A COMPARATIVE ANALYSIS OF PERSONAL DATA PROTECTION BILL 2019 VIS-À-VIS INDIAN PRIVACY JURISPRUDENCE

*Lakshya Sharma*[*] *& Siddharth Panda*[#]

**ABSTRACT**

*The modern-day digitization of elements of data has stirred a debate concerning the moral clash between the state utilitarianism and an individual's right to privacy. Scholars are apprehensive of the current progression which could further lead to the political state of 'Orwellian Dystopia' – created by George Orwell in his creation '1984'. It refers to an autocratic state which is being operated using draconian policies of disinformation, crowd manipulation, and state surveillance.*

*In light of fostering the right to privacy, the Indian government introduced the Personal Data Protection Bill 2018 drafted by the Justice BN Srikrishna Committee. It aimed to strengthen an individual's inherent right to privacy by bestowing control over their personal and private data. However, the Indian government reintroduced the Bill in 2019 with substantial changes to the*

[*] The author is a fourth year student at National Law University, Odisha, and may be contacted at **lakshay6521[attherate]gmail[dot]com**.
[#] The author is a fifth year student at National Law University, Odisha, and may be contacted at **siddharth[dot]panda1997[attherate]gmail[dot]com**.

*erstwhile draft Bill. Thenceforth, it has been heavily criticized because it allegedly undermines potential privacy concerns and compromises the very essence of the interpretative advances made in the Supreme Court judgement of Justice KS Puttaswamy (Retd.) v. Union of India.*

*On the aforementioned premise, the authors attempt to bring conceptual precision to the discourse; firstly, by identifying the roots of 'privacy' in the common law jurisprudence, and secondly, through a comparative analysis of Personal Data Protection Bills 2018 and 2019 on the altar of Indian privacy jurisprudence. The authors also suggest certain policy changes to bring the challenges of state security and right to privacy to a legitimate equilibrium.*

## TABLE OF CONTENTS

## I. INTRODUCTION

In an age where digital surveillance was increasingly becoming the *modus operandi* of the government-corporate complex, popular concern for its informational privacy did not seem to match the hype around it. An average citizen considered such a phenomenon a myth of the future; something that could not be possible today. The indication of such an occurrence in George Orwell's '1984' was well appreciated but considered a work of fiction nonetheless. While the world was facing existential challenges of its own, privacy seemed to be a lesser concern for the general population of India, until, WhatsApp rolled out its updated privacy policy.

WhatsApp is, inarguably, the most popular internet messaging application with a clientele of 1.5 billion active users. It promised seamless interactivity on its platform with end-to-end encryption which assured the users about the security of their data. But everything changed when WhatsApp came out with its 'take it or leave it' policy which would allow it to share 'certain' user information with its parent company, Facebook. Facebook is infamous for allegations of large-scale data breach and info-manipulation. This stirred the pot of popular anxiety about their personal information and data. The clueless public is now frantically trying to comprehend the meaning and scope of a moniker which was casually thrown around but never truly understood: 'privacy'. They look around only to find that the lawmakers are also as clueless as they are. Without any tangible framework to address the concerns of privacy and its protection, India finds itself stranded in an unlimited space of uncertainty. This article

is an effort to clear to haze around the complexity of the issue and provide a context to the problem, if not the solution.

The authors have attempted to highlight the past, present and the possible future of informational privacy and data protection against the threats of digital surveillance, using the notion of 'Orwellian Dystopia' as an anchor to the arguments herein. The authors have traced the jurisprudence of informational privacy, its origin, being and recent developments to highlight how it has influenced the discussion around privacy in India and the world. The authors ultimately put forth an analysis of the Personal Data Protection Bill, which has extensive ramifications for the politico-economy status quo, industry and India's diplomatic standing. While this Bill is hailed by different sections of the industry and political society as the vanguard against 'data imperialism', its vulnerabilities are too patent to be left alone. Thus, the authors have critically analyzed the bill against its vision of security and welfare, and proposed ways to prevent the perils of moral hazard.

## II. THE EVOLUTIONARY JURISPRUDENCE OF PRIVACY

The word 'privacy' finds its etymological roots in its Latin predecessor '*privātus'* which means 'set apart' or 'being single' in its original archaic standard. Later use of the word signified 'which is peculiar or one's own' - the contextual setting evolving from a solitary person to a person relative to the property of other persons.[1] Even today, when we incorporate privacy in a discourse, it signifies a co-relation to the property (or rights) of

[1] Jack Hirshleifer, 'Privacy: Its Origin, Function, and Future' (1980) 9 Journal of Legal Studies 649.

others. Even so, when did the right to privacy rise as a cultural, social and eventually a legal thought?

The earliest argument about privacy as a right could be traced back to S. Warren and Louis Brandeis's seminal work on 'The Right to Privacy'.[2] They contended that protection of privacy should be manifested as a right enforced by law to ensure and protect people's 'involatile personality'.[3] They also contemplated a new way to deal with it as a matter of law, through a specific privacy tort. However, they did not suggest that they were engaging in the invention of some new right. They suggested that the notion of protection of individual rights over one's property (which included the individual itself) was well-founded in common law jurisprudence and demanded that social and political changes be undertaken to acknowledge these rights.[4]

The American Fourth Amendment and its constitutive case of *Entick v. Carrington*[5] provided a preface to the notion of 'privacy' as identified by Brandeis and Warren. Eventually, the authors' broad interpretation of a right to privacy developed as a constitutional bulwark in *Olmstead v. United States*.[6] Therein, the American Supreme Court referred to the right as "*protection against such invasion of 'the sanctity of a man's home and the*

---

[2] Samuel D Warren & Louis D Brandeis, 'The Right to privacy' (1890) 4 Harvard Law Review 193; Louis Nizer, 'Right of Privacy-A Half Century's Developments' (1940) 39 Mich L Rev 526.
[3] ibid.
[4] Michaela Hailbronner, 'Constructing the Global Constitutional Canon: Between Authority and Criticism' (2019) 69 University of Toronto Law Journal 248.
[5] [1765] EWHC KB J98.
[6] 277 US 438 (1928).

*privacies of life', a protection provided for in the Fourth amendment 'by specific language"*'.[7]

By 1905, the right to privacy or the 'right to control information about oneself' was acknowledged and expanded. It also paved the way for segregation of right to privacy from right to liberty, and right to property.[8] Hence, they invented the new concept which protected an 'unprotected' legal right, i.e., informational privacy, meaning control over the information about oneself.[9] Thereon, informational privacy became a talking point across various jurisdictions of the world. These deliberations increasingly gained popularity and priority after the technological boom in the late 20th century. The notion of privacy and its protection has since followed differential trajectories in comparative jurisdictions of USA and European Union which has influenced the global outlook in more ways than one.

### A. AMERICAN JURISPRUDENCE

The right to privacy is not enunciated in the American Constitution or the United States (US) Bill of Rights.[10] The framers of the American Constitution entrusted the states and their social dominion to deal with the matters of privacy, with the significant special case of the Fourth Amendment, which controls and protects people from unreasonable state

---

[7] ibid 473.

[8] Edward Keynes, *Liberty, Property, and Privacy: Toward a Jurisprudence of Substantive Due Process* (Penn State Press 2010).

[9] J Van den Hoven, M Blaauw, W Pieters & M Warnier, 'Privacy and Information Technology', *The Stanford Encyclopedia* (2014) <https://stanford.library.sydney.edu.au/archives/sp r2017/entries/it-privacy.> accessed 30 October 2020.

[10] Michael Birnhack, '*Reverse Engineering Informational Privacy Law*' (2013) Yale JL & Tech 15(1/3) <https://digitalcommons.law.yale.edu/yjolt/vol15/iss1/3> accessed 30 October 2020.

searches and seizures.[11] Privacy was additionally ensured by means of other lawful rights, for example, the right to private property and the copyright law which protects creativity rights and unpublished works.[12] However, the American jurisprudence relating to right to privacy evolved multifariously.

*Firstly*, the privacy hypothesis by Warren and Brandeis was followed by another canonical work by William Prosser which uniformly characterized and arranged the assortment of torts relating to privacy that Courts had come to identify.[13] According to Prosser, privacy torts involved certain invasions into an individual's interests:[14]

> "*(1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;*
>
> *(2) Public disclosure of embarrassing private facts about the plaintiff;*
>
> *(3) Publicity which places the plaintiff in a false light in the public eye; and*
>
> *(4) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.*"[15]

Even though he regularly expressed that his strategies were those of a sampler and a synthesizer as opposed to a pundit or scholar, Prosser held a normative perspective on privacy that affected the manner in which

---

[11] ibid.
[12] ibid.
[13] Bart van der Sloot, 'Privacy from a Legal Perspective' in Van der Sloot, B & A de Groot (eds), *The Handbook of Privacy Studies* (Amsterdam University Press 2018) 63-136.
[14] William L Prosser, 'Privacy' (1960) 48 Calif Law Rev 383.
[15] ibid.

he arranged the privacy torts. Consequently, Prosser attempted to shape the future course of privacy law in a more restrictive and cautious way.[16]

*Secondly*, privacy law evolved through the US Bill of Rights, especially the Fourth Amendment. For over 100 years, the Fourth Amendment was elucidated to forbid state intrusion into private places as opposed to a general provision of the right to privacy. Nonetheless, its understanding evolved parallel to the development of common law to put more prominence on ensuring an individual's personal information.[17] More specifically, the Supreme Court of the United States (SCOTUS) in *Katz v. US*[18] clarified that the Fourth Amendment, while not emphasizing on right to privacy, regardless safeguards individuals, not places, and also protects personal information against certain kinds of state intrusion. This ratio has developed significantly to protect a person's digital privacy to a certain extent.[19] For another instance, in *Carpenter v. US*[20] ("*Carpenter*"), the SCOTUS reasoned that the protection of individual privacy afforded in the Fourth Amendment extends to protect personal data from state interference even where that data was imparted to an outsider or a third party. *Carpenter* differed from Court precedents which had pronounced that data imparted to a third party was not to be protected by the Fourth

[16] Neil M Richards & Daniel J Solove, 'Prosser's Privacy Law: A Mixed Legacy' (2010) 98 Calif L Rev 1887.
[17] Stephen P Mulligan & Chris D Linebaugh, 'Data Protection Law: An Overview' *Congressional Research Service* (25 March 2019) <https://fas.org/sgp/crs/misc/R45631.pdf> accessed 23 February 2021.
[18] 389 *US* 347 (1967).
[19] Helen Nissenbaum, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' (1998) 34 Law and Philosophy 559-596.
[20] 201 L Ed 2d 507.

Amendment. It held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [his cellular phone]."[21] Ergo, the Fourth Amendment has evolved to provide a restricted defence against government interruption into digital information of an individual.

*Thirdly*, a form of privacy protection also developed through American constitutional law. In *Griswold v. Connecticut,*[22] the SCOTUS safeguarded a wedded couple's entitlement to get information and guidance about contraceptive medication, and in the process declared that the notion of privacy is integral to the Constitution even though it has not been explicitly stated therein. Justice Douglas upheld the right to privacy as "*being older than the American Bill of Rights*". In *Whalen v. Roe*[23] ("*Whalen*"), the SCOTUS clarified that the constitutional right to privacy comprises interests of two kinds: "*One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions*."

Unfortunately, despite its expansive articulation in *Whalen*, every SCOTUS judgement thenceforth has consciously rejected the notion of informational privacy as a constitutional right and buttressed state programmes asserted to have encroached on the right.[24] Ergo, American

---

[21] ibid 12.
[22] 381 US 479, 1965.
[23] 429 US 589 (1977).
[24] Fred H Cate & Beth E Cate, 'The Supreme Court and Information Privacy' (2012) 4 *International Data Privacy Law* 255–267 <https://doi.org/10.1093/idpl/ips024> accessed 23 February 2021.

privacy law stayed inside limitedly explicit segments.[25] Even in 2011, the SCOTUS in *NASA v. Nelson*[26] ("*NASA*") assumed that the Constitution safeguards an "*interest in avoiding disclosure of personal matters*", but Justice Scalia simultaneously explained that "*there is no constitutional right to 'informational' privacy*".

Besides the development in common law and American constitutional law, Congress has put efforts to provide a legislative 'patchwork' to the right to privacy, yet the rules are restricted to specific sectors and industries enumerated in the statute.[27] Despite the universal acceptance of informational privacy, the US has adopted a restricted system for privacy protection. The US still relies on self-regulatory guidelines within industry and government. It is evident that the US is still following the laissez-faire approach for protecting informational privacy.[28]

### B. EUROPEAN JURISPRUDENCE

The European Union (EU) law, created and developed by the EU Commission, is the cornerstone of EU legal anatomy. Additionally, two Courts having unique jurisdiction to authorize human rights treaties, i.e., the European Court for Human Rights (ECtHR) for the European Convention on Human Rights (ECHR) and the Court of Justice of the European Union (CJEU) for the EU Charter of Fundamental Rights (CFR),

---

[25] 389 US 347 (1967).
[26] 562 US 134 (2011).
[27] Edward R Alo, 'EU Privacy Protection: A Step towards Global Privacy' (2013) 22 Mich St Int'l L Rev 1095.
[28] Himanshu Dhandharia, 'Developing A Jurisprudence of Privacy in The Digital Era' (2019) 7 Int J Rev and Res Social Sci 353.

transform this setup into a concrete privacy-safeguard system with considerable constraints.[29]

The Organization for Economic Cooperation and Development (OECD) published its 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' in 1980 to establish a homogenous system of data protection mechanism among the member states.[30] Then in 1981, the Council of Europe ("CoE") came up with the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("Convention"). The Convention was additionally moored in the ECHR 1950; the main legal instrument of the CoE. Article 8 of the Convention bestows upon the individual a right to respect for his private and family life.[31] The ECtHR recognizes explicit rights with respect to information privacy based on Article 8:[32]

Article 8 – "*Right to respect for the private and family life:*

> *(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime,*

---

[29] Stephen J Schulhofer, 'An international right to privacy? Be careful what you wish for' (2016) 14 International *Journal of Constitutional Law* 238.
[30] Michael Birnhack, 'Reverse Engineering Informational Privacy Law' (2013) 15 Yale JL & Tech 3.
[31] ibid.
[32] Convention for the Protection of Human Rights and Fundamental Freedoms 1950, art 8.

> *for the protection of health or morals, or for the protection of the rights and freedoms of others.*"[33]

This right is directly and legitimately enforceable in the ECtHR. This clearly showcases the European standards of privacy protection has more explicit textual support and robust framework than the American right to privacy as pronounced through *NASA* and *Whalen*; it is more extensive and profound, shielding more data from less serious intrusions.[34]

CJEU case laws dealing with Article 8 of the CFR offer significant insight regarding EU standards of privacy. In one of its initial pronouncements, in *Rechnungshof v. Oster Reichischer Rundfunk*,[35] the CJEU held that "*the mere recording by an employer of data by name relating to the remuneration paid to employees cannot constitute an interference with private life*". The CJEU observed that this act of recording is "*personal data processing*" and would concern data protection rules. It is quite noticeable that for this case, the CJEU expressly made reference to Article 8 and 52(1) of the CFR which acknowledges that restrictions might be applied on CFR rights, as long as they are provided by law, regard the quintessence of those rights, and are proportionate. The judgement in *Leander v. Sweden*[36] ("*Leander*") likewise showcases the noteworthy standard of EU protection of privacy. Although the CJEU pardoned the state intrusion, it applied a three-section test with respect to permissible grounds of encroachment: *"(a) In pursuit of a legitimate*

---

[33] ibid.
[34] Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 NYUL Rev 771.
[35] C-465/00, [2003] EU ECJ C-465/00.
[36] [1987] 9 EHRR 433, 9248/81.

*interest (here, national security); (b) In accordance with the law; and (c) Necessary in a democratic society*".[37]

Clearly, the CJEU went past the available text to make sure that individuals would be cautioned in an event in which their data may be gathered, monitored or unveiled if their act doesn't warrant or trigger such disclosure (through the test laid in *Leander*).[38] CJEU presumed that the protection of individual information and the respect to private life were so important that the discretion of the legislature of EU would be diminished, and any impedance to rights contained under Article 8 of the CFR must be restricted to cases in which such intrusion becomes necessary.[39]

However, the most notable development in international privacy jurisprudence took place on 25 January 2012 when the European Commission proposed a change in the EU Data Protection regime through the General Data Protection Regulation (GDPR) so as to reinforce digital information privacy rights and augment the digital economy of the EU. It was likewise drafted to adjust to innovative developments that had happened in the earlier decade.[40]

Under Article 4(1) of the GDPR, 'personal data' is defined as:

"*[A]ny information which could be utilized, in itself or concurrent to other information, to identify a person directly or indirectly, specifically by*

---

[37] ibid.
[38] Timothy Azarchs, 'Informational Privacy: Lessons from Across the Atlantic' (2013) 16 U Pa J Const L 805.
[39] ibid.
[40] Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What it is and What it Means' (2019) 28 Information & Communications Technology Law 65.

> *reference to an identifier, for example, a name, a recognizable unique number of identification, area information, an online identifier or to at least one components explicit to the physiological, physical, mental, hereditary, monetary, social or cultural character of that individual.*"[41]

Under the GDPR, personal data or information which incorporates data pertaining to geo-location, IP address, biometric data, for example, unique fingerprint scans, and retina checks, which is a lot more extensive than imagined in its outdated predecessor, the Data Protection Directive (Directive).[42] Second, the GDPR places a noteworthy emphasis on an individual's consent. The GDPR requires unequivocal consenting for the processing or handling of any personal information. The GDPR also aims to put an end to complicated user agreements with complex language that clients seldom read; such description must be short, coherent and direct. A third key distinction between the Directive and the GDPR is that under the GDPR both data processors and data controllers will be mutually held accountable for compliance with data protection rules. At last, the GDPR presents certain novel information rights, for example, right to data portability, which was not present under the Directive.

Article 5 of the GDPR comprises seven key principles, which has been introduced to guide how personal data can be handled. These seven

---

[41] General Data Protection Regulations 2018, art 4(1).

[42] Privsec Report, 'The Data Protection Directive Versus the GDPR: Understanding Key Changes' *Privsec* (6 March 2018) <https://gdpr.report/news/2018/03/06/data-protection-directive-versus-gdpr-understanding-key-changes> accessed 23 February 2021.

principles are: "*(1) lawfulness, (2) fairness, (3) transparency, (4) purpose limitation, (5) integrity, (6) security and (7) accountability.*"[43]

The GDPR ensures that data protection safeguards are inculcated into goods and services from the initial phase of development, ensuring 'data protection by design' in new goods.[44] Customers are ensured uncomplicated access to their personal information to the extent that the organizations dealing with it shall detail how they use the customer information sensibly and reasonably.

## III. A COMPARATIVE ANALYSIS OF THE PERSONAL DATA PROTECTION BILL 2018 AND 2019 ON THE ALTAR OF PRIVACY JURISPRUDENCE IN INDIA

The last couple of years have seen a formalization of the right to informational privacy in the constitutional framework of India.[45] The testing of the legitimacy of the Aadhaar venture has involved more extensive issues on the conveyance of information and privacy. The reaction to whether an individual can affirm command over important informational factors of his/her life has become an intrinsic portion of our rights and privacy jurisprudence.[46]

---

[43] General Data Protection Regulations 2018, art 5.

[44] Danny Palmer, 'What is GDPR? Everything you need to know about the new general data protection regulations' *ZDNET* (17 May 2019) <https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/> accessed 23 February 2021.

[45] Anirudh Burman, 'Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?' *Carnagie* (9 March 2020) <https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217> accessed 23 February 2021.

[46] ibid.

### A. INDIAN PRIVACY JURISPRUDENCE

The Personal Data Protection Bill 2019 follows a long queue of events in Indian privacy jurisprudence impacted by international developments as well as Indian constitutional evolution. The Constitution of India 1950 ("Constitution") does not unequivocally refer to one's right to privacy. However, Indian courts, through a series of pronouncements, have held that a right to privacy exists under the right to life and liberty ensured under Article 21 of the Constitution. However, there was always some vagueness in regard to the constitutional protection to privacy rights because of the continuous precedence of *Kharak Singh v. State of Uttar Pradesh*[47] ("*Kharak Singh*") and *MP Sharma v. Union of India*[48] ("*MP Sharma*"), wherein the Supreme Court of India ("SC") held that the right to privacy did not exist under the Constitution.

It should be acknowledged that smaller benches of the SC had indirectly affirmed that the Constitution protects the right to privacy in *Gobind Sharma v. Union of India*[49] and *R Rajagopal v. Union of India.*[50]

However, it was in *PUCL v. Union of India*[51] ("*PUCL*"), where the SC laid the modern foundation of the privacy rights jurisprudence in India with regard to informational surveillance (telephone tapping). The SC herein scrutinized the constitutional legitimacy of Section 5(2) of the Indian Telegraph Act 1885 ("IT Act") which granted unbridled power to the state

[47] 1964 SCR (1) 332.
[48] 1954 SCR 1077.
[49] (*1975*) 2 SCC 148.
[50] 1994 SCC (6) 632.
[51] (1997) 1 SCC 301.

to intercept in a situation of public emergency or in the interest of public safety. Interestingly, these two terms were not defined in the IT Act. This paved way for extensive use of this unlimited power by the enforcement agencies based on the subjective satisfaction of the central/state government(s). While the SC took notice of the conundrum, it did not declare the provision as unconstitutional. Yet, it laid down the 'two-way test' which must be satisfied to exercise this power of interception:

> A) The statutory pre-conditions of public emergency and public safety shall be read and interpreted in their entirety for they "*take colour*" from one another.[52]
>
> B) The SC interpreted public emergency to incorporate situations concerning "*the interest of public safety, the sovereignty and integrity of India, the security of the State, friendly relations with foreign states, public order, or the prevention of incitement to the commission of an offence*"[53] only. As none of these situations is secretive in nature, it should be apparent to a reasonable person.[54]

Additionally, the SC held that economic emergency does not meet the criteria of public emergency, and along these lines, an interruption for the mitigation of economic offences does not qualify the exceptionally high parameters of public emergency or public safety.

Now, the most important development in Indian privacy jurisprudence occurred when a nine-judge bench of the SC bestowed

---

[52] ibid 314.
[53] ibid.
[54] ibid.

unequivocal constitutional legitimacy to right to privacy by overruling *MP Sharma* and *Kharak Singh* and subjecting the pronouncements therein to the highest level of judicial scrutiny.

Founded on the premise that "privacy is the ultimate expression of the sanctity of the individual", the Supreme Court differentiated from the pre-existing privacy jurisprudence on two grounds in *Justice KS Puttaswamy (Retd.) v. Union of India*[55] ("*Puttaswamy*"). *Firstly*, it distinctly and unambiguously expressed that the fundamental right to privacy is inherent to the Constitution. *Secondly*, the more critical ground was that the right to privacy was conceptualized as a 'right in itself', and as such, mandated its own protection. Significantly, this understanding of privacy rights works parallel to the internationally existing frameworks which deal with informational privacy. The test of proportionality and legitimacy was likewise settled and elaborated as a four-crease test that should be satisfied before any sort of state intrusion is permitted.

Most recently, the Bombay High Court dealt with a case relating to surveillance and telephone tapping in which it scrutinized Section 5(2) of the IT Act on the altar of *Puttaswamy*.[56] Herein, a businessperson had allegedly offered payoffs to bank officers to get illegitimate financial credit. He challenged certain orders of the Central Bureau of Investigation, which attempted to tap his calls, on the ground that these aforementioned orders were *ultra-vires* Section 5(2). The High Court in its judgement reiterated the 'two-way test' established by the SC in *PUCL*. Thenceforth, in light of the

---

[55] (2017) 10 SCC 641.
[56] *Vinit Kumar v Central Bureau of Investigations and Ors* [2019] ALLMR (Cri) 5227.

settled positions, the High Court held that there is no clear public emergency or safety factor to justify the said orders and it doesn't fulfil the test on the principles of proportionality and legitimacy as set out in *Puttaswamy*.

In summary, the *Puttaswamy* judgement has hailed reasonability as the saviour of right to privacy'. It draws a lakshman-rekha around the right which could only be breached if the concern is legitimate and rightful in the eyes of law and logic. This paves the path for rare policy equilibrium where a citizen's individual and collective rights could complement each other.

### B. THE WHATSAPP CONTROVERSY

In January 2021, WhatsApp rolled out its controversial '*take it or leave it*' privacy policy raising serious privacy concerns for the Indian sub-continent. Users were given an option either to accept it or lose access to their accounts. The social media giant received huge backlash from the Indian users in the form of them migrating to other platforms. In light of the transpired event, WhatsApp put a hold on the policy till 15 May 2021.

Highlighting the absence of any concrete legislation in place to deal with such situations, WhatsApp took it as a defence before the SC. However, the SC noted that had the proposed Personal Data Protection Bill 2019 ("PDP Bill") been in place, WhatsApp would have faced serious repercussions for such measures.[57] Although the matter is *sub judice*, it

[57] Anumeha Chaturvedi, 'Supreme Court issues notices to Facebook, WhatsApp over new privacy policy' *Economic Times* (16 February 2021) <https://economictimes.indiatimes.com/tech/technology/supreme-court-issues-notice-to-govt-whatsapp-on-plea-overprivacy-standards/articleshow/80920387.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst'> accessed 23 February 2021.

becomes quintessential to analyse the provisions of the PDP Bill alongside the controversial WhatsApp Privacy Policy as to determine whether the PDP Bill is equipped to deal with such situations.

### i. Valid Consent and Purposive Limitation

As per Section 11(4) of the PDP Bill, for consent to be valid for the quality and provision of services, it should be linked to consenting only to the purpose which is primary and not incidental. Further, Section 5 provides that personal data shall only be processed "*for the purpose consented to by the data principal*".[58] This provides a purposive limitation to the processing of data.

In the case of WhatsApp, the primary purpose is to process data in order to provide messaging and communication services. Sharing the personal data with Facebook or third-party service providers for better marketing or better integration of their services is incidental in nature. Forcing the users to either accept the terms or switch to other platform is tantamount to invalid consent in the present context. Additionally, the same violates the provisions of purposive limitation - another principle adopted from GDPR[59] - since the policy deviates from its primary or specified purpose.

### ii. Privacy Notice

As per Section 7, an obligation is placed on the data fiduciary (i.e., WhatsApp) to provide a notice of privacy containing intricate and essential

[58] Personal Data Protection Bill 2019, s 5.
[59] General Data Protection Regulations 2018, art 5(1)(i).

details about processing the personal data of the data principals (i.e., users).[60] The details are to be provided in an unambiguous, comprehendible and concise manner. Further, the policy is to be provided in multiple languages so as to cater the needs of larger audience.

The WhatsApp policy is unable to fit into these descriptions as *firstly*, the text-based policy runs into 3800 words and without in a layered format thereby making it incomprehensible to an extent.[61] *Secondly*, the policy uses vague terms in relation to data processing and can lead to different interpretations. *Lastly*, the current policy is based out in English and hence reduces the reach of people. Hence, WhatsApp defaults at giving a proper privacy notice.

### iii. Rights of Data Principals

As mentioned previously, the PDP Bill is inspired greatly by the GDPR. The GDPR provides for users to exercise their rights as 'data principals' in the form of right to access,[62] rectification,[63] port,[64] and erase their information,[65] as well as, the right to restrict[66] and object to certain processing of their information.[67] The PDP Bill borrows such rights of data principals and has incorporated the same in the proposed framework. As

---

[60] Personal Data Protection Bill 2019, s 7.
[61] 'WhatsApp Privacy Policy' *WhatsApp* (4 January 2021) <https://www.whatsapp.com/legal/updates/privacy-policy?lang=en> accessed 23 February 2021.
[62] General Data Protection Regulations 2018, art 15.
[63] ibid art 16.
[64] ibid art 20.
[65] ibid art 17.
[66] ibid art 18.
[67] ibid art 21.

per Section 17,[68] data principals have the right to confirmation and access. Section 18 empowers data principals with right to correction and erasure and Section 19 gives data principals a right to data portability.[69]

In the present case, WhatsApp has set out to share its users' data with Facebook and third-party service providers for different uses. However, the policy is silent on the identity of third-party service providers and the categories of data to be shared.[70] As per the PDP Bill, the data principal has a right to be informed and right to provide consent about the individuals or entities that requires the consent.[71] Therefore, the current policy is in clear breach of the right of data principal provided under the PDP Bill.

If the PDP Bill becomes an act, WhatsApp will have to make significant amends to its current policy by incorporating the rights of data accorded to data principals. Although, the current framework provided considerable protection from such unjust policies, the PDP Bill has some shortcomings that again raises the question over right to privacy. The authors have drawn a comparative analysis of the 2019 PDP Bill with the 2018 Personal Data Protection Draft Bill and highlighted the gaps where the concerns for privacy lies.

---

[68] ibid art 17.
[69] ibid art 18 and 19.
[70] WhatsApp (n 57).
[71] Personal Data Protection Bill 2019, ss 17(3) and 7(1)(g).

## C. A COMPARATIVE ANALYSIS OF THE 2019 PDP BILL VIS-À-VIS THE 2018 DRAFT BILL

The SC in *Puttaswamy* recommended the Union Government to develop "*a robust regime for data protection balancing individual interests at one hand and legitimate state concerns on the other*".[72] The Indian Government in its response to strengthen the regulation and collection of personal data of the citizens tabled the PDP Bill, which is now under the consideration of the Parliament. Upon its approval, the PDP Bill shall stem the foundation of privacy laws across the country and will govern the personal data being monitored and solicited by entities which collect and process the data in order to meet their business motives.

The Expert Committee on Data Protection led by Justice Srikrishna categorically stated in its report, "*a data protection law, to be meaningful should, in principle, apply to the State. It would indeed be odd if a law enacted to give effect to a fundamental right to privacy does not serve to protect persons from privacy harms caused by processing of personal data by the State.*"[73] The PDP Bill is an extension of the erstwhile Personal Data Protection Bill 2018 ("2018 draft Bill") proposed by the Justice BN Srikrishna Committee ("Srikrishna Committee").[74] However, the PDP Bill as introduced before the Parliament differs substantially from the Srikrishna Committee's draft.

---

[72] ibid s 273.
[73] Justice BN Srikrishna Committee of Experts, *Report of the Committee on Data Protection – A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology 2018) 114 ("2018 Report").
[74] ibid.

The PDP Bill introduces new concepts and deviates from the 2018 draft Bill in certain aspects. One of the key deviations includes the blanket and unaccountable powers bestowed upon the Central Government to process the data which calls for the question of privacy. The following are certain junctures through which it can be ascertained how the PDP Bill dilutes privacy:

### i. The PDP Bill empowers the state with *carte blanche*

The PDP Bill empowers the Central Government to give directives and exempt government agencies from the reaches of the PDP Bill on the wide grounds of national security, sovereignty, and public order.[75] This is a stark deviation from the 2018 draft Bill, wherein such an exemption could only be availed in the name of national security when the same pass the contours of law enacted by the Parliament, provided it meets the standards of internationally recognized principles of necessity and proportionality.[76]

As per Section 35, a mere executive order will suffice to "*authorise any government agency to process personal data and allow them to conduct surveillance without any clear safeguards*".[77] The Srikrishna Committee had strongly recommended that such exemption should only be provided through the law. However, such deviation can be seen as a conscious attempt to interfere with the right to privacy of the citizens.

Additionally, the blanket powers enshrined upon the state under the guise of these exemptions fail to qualify the test laid down in *Puttaswamy* as

---

[75] Personal Data Protection Bill 2019, s 35.
[76] *Puttaswamy* (n 55) 71 (Per SK Kaul, J).
[77] Personal Data Protection Bill 2019, s 35.

per which the right to privacy can be curtailed only through the law to serve a legitimate aim, while being proportionate to the objective of the law, and having procedural safeguards against the abuse. However, the PDP Bill widens the scope of these exemptions by doing away with the test laid down in *Puttaswamy* and thereby poses a serious threat to the right to privacy having far-reaching consequences. It is undisputed that national interests may override the individual's privacy, but the threshold should be high, as Justice Srikrishna Committee noted, "*to ensure that the pillars of the data protection framework are not shaken by a vague and nebulous national security exception*".[78]

### ii. Impeding with the Independence of Data Protection Authority

The PDP Bill abrogates powers of the Data Protection Authority ("DPA"), to be created, under its aegis. The erstwhile 2018 draft Bill provided for the powers and functions of the DPA, which do not find a place in the current PDP Bill presented by the Central Government before the Parliament.[79] This creates an imbalance in the whole mechanism of data collection and processing, and indirectly raises the pedestal of the state in privacy matters. The 2018 draft Bill empowered the DPA with distinct regulatory powers:

---

[78] Renjith Mathew, 'Personal Data Protection Bill, 2019 – Examined through the Prism of Fundamental Right to privacy – A Critical Study' *SCC Online* (22 May 2020) <https://www.scconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/#_ftn30> accessed 23 February 2021.

[79] 2018 Report (n 73) 181.

(i) The DPA, under the 2018 draft Bill, was the competent authority to notify the categorisation of sensitive personal data whereas now, as per the PDP Bill, the power to notify vests with the Central Government who can do so in consultation with the sector regulators.[80]

(ii) Furthermore, the DPA, under the 2018 draft Bill, had the primary authority to decide, identify and notify data fiduciaries. However, as per the current PDP Bill, the Central Government has taken up that role in consultation with the DPA by relocating the latter from the primary source to the secondary.[81]

### iii. "The Big Brother Is Watching You"

The PDP Bill prescribes that "*the procedure, safeguards and oversight mechanism to be followed for surveillance shall be notified via rules framed by the Government*". However, no clear and specific guidelines have been provided in the PDP Bill in relation to the same, which thereby gives excessive and wide discretionary to the executive wing of the government. The delegation of such important powers solely to the government further precludes the role of legislature and rules out the possibility of any parliament debate.

The PDP Bill is inspired significantly by the GDPR which also empowers the EU member states with similar escape clauses. But, at the same time, they are subjected to other EU directives. In absence of these safeguards, the PDP Bill gifts unbridled authority to the government

[80] ibid 175.
[81] ibid 167.

through which it can access individual data over and above the existing laws, breaching the four-fold test laid out in *Puttaswamy*.

### iv. The Conundrum revolving around the Non-Personal Data

The PDP Bill introduced a new provision for the government-mandated processing and sharing of privately collected and solicited non-personal data.[82] It further empowers the government to formulate policies for the digital economy in relation to non-personal data.[83]

As per Section 91(2), "*the government may direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government*".[84] This is a clear deviation from the 2018 draft Bill where under Section 105, it was categorically stated that policies formulated under it would not govern non-personal data.[85]

The abovementioned addition to the PDP Bill calls for serious deliberation and reconsideration. *Firstly*, no reasonable explanation has been provided as to why a bill dealing with personal data protection includes non-personal data in its purview. *Secondly*, no definition has been provided to the said term under the definition clause and furthermore, this provision does not even enable any mechanism through which the government would process such data. It can be said, under this provision, the Central Government has the requisite power to commandeer

[82] Personal Data Protection Bill (2019), s 91.
[83] ibid.
[84] ibid s 91(2).
[85] ibid s 105.

intellectual property which could have far-reaching consequences on the incentives on innovation in the long run.

### v. Anonymisation of Data

Data anonymisation alludes to an irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified.[86] It further prescribes for an irreversible method of data anonymisation specified by the authority.[87] However, research findings across the world show that irreversible anonymisation is improbable.[88] The PDP Bill has no mention of the standards for the data anonymisation and penalties for any breach, thereby leaving wide scope for the state to invade privacy of the people by accessing their anonymised personal data.

## IV. A KEY TO THE CONUNDRUM: REMARKS AND RECOMMENDATIONS

In the previous sections, we saw how significant changes and modifications were brought to the PDP Bill to make it in tune with the government's policy. However, the PDP Bill's objective was to empower citizens and concretise the state's role in ensuring their privacy, but it falters at both junctures. These modifications, as discussed already, have the requisite potential to jeopardise the privacy of individuals by concentrating such unaccounted and unfettered powers in the hands of government. The committee led by Justice BN Srikrishna made sure that all the provisions of

---

[86] ibid s 3(2).
[87] ibid.
[88] Sophie Stalla-Bourdillon and Alison Knight, 'Anonymous Data v Personal Data - A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2017) 17 Wisconsin International Law Journal 6.

the 2018 draft Bill were aligned with the decision of the SC in *Puttaswamy*. The moves of the state, with the introduction of the PDP Bill, are apprehensive of potential rights intrusion which could put Indian Constitutional values at stake.

The authors strongly proscribe the intent shown by the Central Government and recommend that all these provisions are to be revisited and remodelled. The authors have analysed and further a few suggestions upon which discussions and deliberations can be done:

### A. REVISITING THE DEFINITION OF 'STATE' AS PROVIDED UNDER THE BILL

State plays a pivotal role when it comes to the collection of personal data of the citizens and under the same, the scope of it should be determined after exercising due care. PDP Bill defines 'state' in the exact words as the term is defined under Article 12 of the Constitution.[89] Article 12 has been defined broadly to impose the 'state' with the widest set of responsibilities and functions vis-à-vis the individual to ensure the constitutional protection of individual rights.[90] However, when this definition is used to curtail the rights of the individuals rather than expanding, then the whole legislative intent behind the wide definition stands vitiated. For instance, Section 12 allows the government to exercise non-consensual processing of data in various circumstances.[91] Given the wide scope of the definition, the provision can be used as a tool by various

[89] Personal Data Protection Bill 2019, s 3(39).
[90] *Pradeep Kumar Biswas v Indian Institute of Chemical Biology* [2002] 2002 5 SCC 111.
[91] Personal Data Protection Bill 2019, s 12.

government entities, coming under the umbrella of Article 12, to restrict individual rights. This further entails that these entities under the garb of the state could avail the option of non-consensual processing of the personal data.

By keeping the above factors into consideration, the authors suggest that the legislature should revisit the definition of the state provided under Section 3(39) of the PDP Bill and remodel it in such a manner that it does not limit the rights of the individuals. At the same time, the scope of the definition should be narrowed down so that it meets the objective set out in the PDP Bill. The test of proportionality should be made an essential threshold to process the data under Section 12 of the PDP Bill which thereby meets the requirements set out in *Puttaswamy* and safeguarding the individual rights of privacy.

### B. DELETION OF SECTION 35 OF THE PDP BILL

As previously discussed, Section 35 empowers the government with a blanket and unaccountable powers to exempt any government agencies or entities from the reaches of the legislation on the broad grounds of national security, sovereignty and public order, if it satisfies the 'necessary and/or expedient' requirements which shall be prescribed by the government in due course. Further, the provision operates outside the realm of judicial oversight and thereby provides the state to ride an unruly horse which has the requisite potential to castrate the rights of the individual to shreds.

By placing reliance on the abovementioned factors, the authors believe that this section should be dropped down in its entirety as it suffers from the vices of lack of transparency and accountability. Furthermore, Section 42 of the 2018 draft Bill, which provided for such exemptions only in the event of national security, subjected to the condition that "*it is authorised pursuant to a law, and is in accordance with the procedure established by such law, made by Parliament and is necessary for, and proportionate to, such interests being achieved*",[92] should be reinstated.

## C. INDEPENDENT DATA PROTECTION AUTHORITY

Bodies such as the DPA, envisaged under the PDP Bill, shoulder bigger responsibilities when it comes to serving national interest as they are vested with obligations to collect and process the inherently sensitive personal data of people. This necessitates the independence of such bodies so that they can render their functions effectively and without being subjugated to anyone.

The authors recommend that the independence of the DPA can be restored in two possible ways:

### i. Composition of Data Protection Authority

As per Section 42 of the PDP Bill,[93] the DPA shall comprise of a chairperson and six whole-time members appointed by the Central Government, thereby eliminating the scope of appointment of any part-

[92] The Wire Staff, 'Final Privacy Bill Could Turn India into 'Orwellian State': Justice Srikrishna' *The Wire* (11 December 2019) <https://thewire.in/law/privacy-bill-india-orwellian-state-justice-bn-srikrishna> accessed 23 February 2021.
[93] Personal Data Protection Bill 2019, s 42.

time or non-executive member. This empowers the Central Government to exercise absolute power in the authority-selection process, unlike the 2018 draft Bill, which recommended a judiciary led selection process.[94] The erstwhile provision dealing with the selection process of the authority in the draft Bill should be reinstated so that a checks-and-balances mechanism can exist, and the executive can transparently render its obligations and functions.

### ii. Powers of the Data Protection Authority

The PDP Bill provides the Central Government with discretion in the categorisation of sensitive personal data and notifying data fiduciaries. Further, as provided under Section 86 of the PDP Bill,[95] the government can issue directives to the DPA on public policy and in the interest of national security and sovereignty. It should be known that the state agencies will be the prime players to be regulated under the proposed law and therefore the discretion lying with the State in such matters interfere with the functional autonomy of the authority.

To maintain the equilibrium and restore the independence of the DPA, it is imperative that these provisions are revisited, and the recommendations of the 2018 draft Bill should be reinstated. The current state of affairs feed the apprehensions of the Srikrishna Committee – the apprehension of the state turning into an Orwellian Dystopia. Such unauthorized and unaccounted power could prove disastrous and detrimental to our cherished constitutional principles and beliefs. In light

[94] ibid.
[95] ibid s 86.

of this, it is strongly recommended by the authors that such unfettered power be ceased, and the PDP Bill be re-amended in accordance with the SC's judgement in *Puttaswamy*.

The aforementioned recommendations might be considered to manage the factors posing a threat to the right to privacy in India. Even though the state may cite problems of state security and surveillance to check potential terrorist activities, the authors in the next section have tried to depict a picture on the premise of Orwell's '1984' to draw a theoretical line of reasoning between an individual's right to privacy and the State's prerogative of surveillance.

## V. THE ILLUSORY NOTION OF PRIVACY IN AN 'ORWELLIAN DYSTOPIA'

The notion about the protection of privacy is founded upon the origination of a person and their interrelation with society.[96] The possibility of public and private circles of activity expects a network wherein such an arrangement is conceivable; however, this positive origination of privacy is an advanced development which came out of a twin development in legal and political thought.[97] The right to privacy was never an absolute privilege, yet, because of the possibility of moral injury, i.e., damage done to one's conscience or moral compass,[98] through privacy violations, right to privacy must be protected by mandating the state and others to justify or legitimize

[96] Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89 The Yale Law Journal 421-471.
[97] Raymond Wacks, *Privacy and Media Freedom* (Oxford Uni Press 2013).
[98] Ferdinand Schoeman, 'Privacy: philosophical dimensions' (1984) 21(3) American Philosophical Quarterly 199-213.

their need to intrude.[99] The age of digitization and the post-internet scope of privacy have left the individuals to care a lot more about their privacy concerns.[100] This warrants an urgent need for more cautious and insightful privacy safeguards and controls pertaining to means of surveillance such as telephone tapping, email hacking, medical reports, scans at the airport, biometric modes of identification, brain scans and other means to decipher and predict an individual's personality and lifestyle choices. As innovation propels, difficulties pertaining to privacy protection will multiply. The legislature, the judiciary, and socio-legal academia must put greater efforts to ensure the protection of personal privacy in these dynamic times.[101]

As per Hubbard, the advanced age of digitization produces a greater chance of unfamiliar privacy harms, considering the extended nature and degree of surveillance, the modern form of peeping is maybe not the same as the physical one:[102]

*Firstly*, there exists a power imbalance in the data surveillance framework. The entities which try to collect information about the individual are, often, more powerful and advanced than the individual.[103] Due to their heightened capacity, they can devise intelligent and secretive means to gather the data, employ individuals to sort and put it in order, and without much of a stretch, share or sell it. Entities with such capability can

---

[99] ibid.
[100] AM Macleod, 'Privacy: Concept, Value, Right?' in A Cudd & M Navin (eds), Core Concepts and Contemporary Issues in Privacy (Springer 2012).
[101] ibid.
[102] P Hubbard, 'The Need for Privacy Torts in an Era of Ubiquitous Disclosure and Surveillance' in A. Cudd & Navin M. (eds), *Core Concepts and Contemporary Issues in Privacy* (Springer 2018) 137-157.
[103] ibid.

likewise misshape reality, mould the truth, and take things outside the realm of relevance, causing it to appear as though one has disclosed one's information, done something wrong, or disregarded a respected belief that could bring cruel repercussions. On the off chance that one becomes a victim of such an attack, one might fear the consequences it may usher.[104]

*Secondly*, the nature of surveillance might be impersonal, as in, the entities might be gathering data about the individual in a reductionist manner; simply a few kinds of information that they care about.[105] This implies the information about the individual is restricted, for example, a website that an individual regularly surfs or a product that an individual purchases. Such generic forms of information can appear as harmless; however, this data can be digitally mined, interconnected across different gadgets and locations, and joined with other forms of personal information about the individual. Besides, this computerized information might be put away in different locations that are latent and obscure to people of humble computational capacity. This implies that the individual or his/her digital signature cannot be forgotten – a mischief empowered by advanced innovations.[106]

*Thirdly*, the use of such personal information could critically hinder the bargaining power of the already deprived consumers in the global

---

[104] A.E. Cudd & M.C. Navin, 'Introduction: Conceptualizing Privacy Harms and Values' in A. Cudd & Navin M. (eds), *Core Concepts and Contemporary Issues in Privacy* (Springer 2018).
[105] ibid.
[106] Macleod (n 100).

market.[107] Economists have analyzed a number of surveys concerning individuals and their business choices, identified with the utilization of personal data, as well as potential forms and impacts of prevailing privacy guidelines.[108] The standard economic analysis of privacy looks at its costs and benefits to different parties in a transaction, and their resulting incentives. Generally, consumers want producers to be acquainted with products and services of their interest; to reduce their own search costs. On the other hand, producers have an incentive to provide this information. However, consumers do not want producers to know how much they are willing to pay. Otherwise, the producer would be empowered to diminish the bargaining power of the consumer by quoting a price as close as the amount each buyer is willing to pay.[109]

With respect to protection of privacy, personal autonomy could be construed as a negative right against the state.[110] Security can be practised, to some evident degree, basically by community watches and self-conservation. Nor is this an insignificant marvel even today, a person who stays inert regardless of assaults of his rights is most likely not going to hold them. Be that as it may, for protecting our privacy, we depend upon the help of law, an arrangement of an outsider definition and execution of

---

[107] Ian Brown, 'The Economics Of Privacy, Data Protection And Surveillance' in *Handbook on the Economics of the Internet* (Edward Elgar Publishing 2016).
[108] Curtis R Taylor, 'Consumer Privacy and the Market for Customer Information' (2004) 35(4) RAND Journal of Economics 631-50 <http://www.jstor.org/stable/1593765> accessed 10 February 2021.
[109] Ian Brown (n 107).
[110] Jack Hirshleifer, 'Privacy: Its Origin, Function, and Future' (1980) 9 Journal of Legal Studies 649-664.

private property rights.[111] Laws can be set up by a general town meeting and maintained by a general show of hands as the need arises. However, our society chooses (or had forced upon itself) the elective arrangement of coercion that is a 'government'. A perilous arrangement, perhaps!

While the world we have come to know is one based on monitoring by privately owned businesses, monetizing and controlling society with no end more than commercial gain, George Orwell had already foreshadowed such reconnaissance and surveillance as the realm of the state in his magnum opus '1984'.[112] Living in a post-Edward Snowden world, security and personal data is a value-based idea.[113] We have been exposed to a greater possibility where we are compelled to exchange our privacy for security and wellbeing, normalizing state surveillance in each aspect of our life, slowly heading towards an Orwellian Dystopia.

Indeed, the concerns surrounding state security and prevention of terrorism are very real and important in the current state of national and international state administration. Would it be a good idea for us to take into consideration reconnaissance innovations in exchange for our fundamental and constitutional rights? We bolster a framework that takes into account this power imbalance between the watchers and the ones being watched. Such advancements must be limited by state policy to be utilized

---

111 ibid.

112 Kalev Leetaru, 'As Orwell's 1984 Turns 70 It Predicted Much Of Today's Surveillance Society' (*Forbes,* 6 May 2019) <https://www.forbes.com/sites/kalevleetaru/2019/05/06/as-orwells-1984-turns-70-it-predicted-much-of-todays-surveillance-society/#5b0e613411de> accessed 10 February 2021.

113 Anthony Berteaux, 'Orwellian Privacy Invasion' *Daily Aztex* (2 October 2014) <http://thedailyaztec.com/57152 /opinion/orwellian-privacy-invasion/> accessed 10 February 2021.

to keep up equity without attacking citizen privileges and freedoms. For police who exist to protect and serve by upholding such technology without a warrant or consent, the vagueness of the morals and power imbalance in the dreaded means of surveillance ought to earnestly concern all of us as we ask more questions – do we feel any safer than before?[114]

We live in a time where a greater portion of ordinary interactions is made through technological means. However, this convenience of sorts comes at incredible expense to our own freedom. Our variants of 'Big Brother' takes several forms; a few, yet not all of them are the organizations of different world governments. The state can effortlessly employ propaganda and surveillance systems that intently look like those of Ingsoc.[115] Recent international events have demonstrated that numerous governments promptly work to censure individuals who exercise free speech and expression. Citizens who publicly reject the state's account face serious repercussions. To summarize Orwell, until we become aware of the manners by which new media is being utilized against us, we will never revolt. Our conscience relies upon the readiness to revolt.

## VI. CONCLUSION

Amidst the WhatsApp controversy, the impending PDP Bill raises multiple red flags over the right to privacy guaranteed under the constitution. The authors argue that the PDP Bill gives unaccountable and absolute powers in the hands of the State while dealing with the sensitive

---

[114] Gavin JD Smith, 'Exploring Relations Between Watchers And Watched In Control (Led) Systems: Strategies And Tactics' (2007) 4 Surveillance & Society 4.

[115] Greg Diglin, 'Living The Orwellian Nightmare: New Media And Digital Dystopia' (2014) 11 E–Learning and Digital Media 6.

personal data of citizens. The wide exemptions provided under the proposed PDP Bill to the state-owned entities in processing such data jeopardize the very tenants of privacy. The authors are of the opinion that such interference with the inherent right to privacy will push for a state of complete surveillance for which a parallel has been drawn with the 'Orwellian Dystopia'.

The PDP Bill is in its final stages and is currently reviewed by a Joint Parliamentary Committee; upon enactment the same shall govern the sensitive personal data of citizens. It is crucial for the legislature to deliberate upon these provisions to make it tune with the fundamental right to privacy envisioned by our forefathers and recognised by the SC.