# CONFIDENTIALITY AND DISSEMINATION OF PRIVATE INFORMATION: AN ANALYSIS OF INDIAN LAWS PERTAINING TO DATA PROTECTION

Aradhya Jain, Army Institute of Law, Mohali

**ABSTRACT**

When a person interacts with a state, that state can accumulate a significant amount of data on that person. There are very little statutory provisions or case laws that prohibit governments from sharing information on their citizens, and any dedicated investigator can find a shocking array of personal data about practically anyone in India without breaking any laws. Currently, there is no explicit legislation in India addressing data protection or privacy. Nonetheless, the Information Technology Act of 2000, The Right to Information Act, 2005, The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and the (Indian) Contract Act of 1872 are the fundamental data protection regulations in India. India's Constitution does not expressly recognize the right to privacy as a fundamental right. However, the courts have incorporated the right to privacy into other existing fundamental rights, such as freedom of speech and expression under Article 19(1)(a) of the Indian Constitution and the right to life and personal liberty under Article 21. It is imperative to notice that Right to privacy under the Constitution of India is subject to reasonable restrictions as held by the Hon'ble Supreme Court in Justice K. S. Puttaswamy (Retd.) & Anr. vs. Union of India and Ors. Another key development in data protection law has been introduction of the Personal Data Protection Bill, 2019 by the Minister of Electronics and Information Technology in the Lok Sabha. The aim of this bill is to provide for the protection of individuals' privacy in relation to their personal data, as well as to establish a Data Protection Authority of India for these purposes and matters relating to an individual's personal data whilst superseding Section 43-A of the Information Technology Act, 2000. From an international approach the EU General Data Protection Regulations have also helped in shaping the data protection provisions and right to privacy in India. This paper primarily aims to promulgate a detailed conception on various statutes and provisions related to data protection as so exists in the Indian legal system.

**Keywords :** data protection, information, confidentiality, data, privacy.

## INTRODUCTION: DATA AS A CONCEPT

Section 2(1)(o) of the **Information Technology Act, 2000 (the "IT Act")** has defines "data" as *"a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."*[1]To put it in a precise manner- Facts gathered by observations or records of events, objects, or people are referred to as data.[2] The Digital Locker Authority's electronic consent framework defines 'data' as any electronic information maintained by a public or private service provider (such as a government service department, a bank, a document repository, etc. Both static and transactional documents can be included in data. Data, on the other hand, is not just limited to electronic information; it also includes information saved in physical form, such as on a sheet of paper.[3]

The number of ways we use data has increased so dramatically in the 21st century that it is now frequently referred to as the "information age." Computers can now process large amounts of data in order to find correlations and patterns in all areas of human activity, thanks to rapid technological advancements. The importance of these databases has been recognized by businesses all over the world, and the technology for mining and utilizing the data available online, is improving every day. Big Data analytics, for example, is being used to analyze incredibly massive and complicated collections of data. Organizations and governments can get extraordinary insights into sectors like health, food security, intelligent transportation systems, energy efficiency, and urban planning by utilizing such analytics. This is a digital revolution in the making.

## THE ORIGIN AND RATIONALE OF DATA PROTECTION

An Individuals' personal information is protected by data protection principles, which limit how such information can be collected, used, and released.[4] Because of the advent of a wide

[1] "Information Technology Act, 2000," 21 of 2000 § (2000),
[2] Clare and Loucopoulos (1987: 2) quoted by Checkland and Holwell (1998).
[3] *"Data-Protection-26-Privacy-Issues-in-India.Pdf,"* accessed August 25, 2021, https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf.
[4] Lee Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits'* 2 (Kluwer Law International: The Hague/London/New York, 2002).

range of issues relating to personal information being processed through automated means, it has grown as a legal right in many jurisdictions of India. In order to comprehend these issues, it is crucial to analyze the use of personal information as a critical activity in society, because it not only provides many benefits but also has the potential to cause severe harm. As a result, the demand for data protection stems from the desire to avoid such harms, and it rests on the question of who should be allowed to use personal data and how.

It's critical to grasp this concept in relation with privacy, because privacy can take on multiple meanings depending on context. ***Spatial privacy*** refers to the privacy of physical spaces, persons, and things; ***Decisional privacy*** refers to the privacy of certain major self-defining choices; and ***Personal Information privacy*** refers to the privacy of personal information (informational privacy).[5] Data protection is generally associated with the concept of informational privacy.[6] The right to privacy is the ability to be alone or to be secure from the misuse or abuse of one's identity. The right to privacy is the right to be free from unwarranted publicity, to live in isolation, and to be free from unwarranted public interference in situations that are not of public importance.[7] However, not all information about a person is private and deserves to be protected by law. It is up to the legal system to decide where such liberty is appropriate and where it is not.

## GENESIS OF RIGHT TO PRIVACY WITH RESPECT TO COMMON LAW

Some features associated to an individual, such as their body, sexuality or ability to form one's own individual characteristics, are extremely vital to one's identity.[8] When it comes to protecting an individual's reputation, privacy is highly valued. Individuals are wrongly stereotyped and prejudged when certain types of controversial and sensitive material is disclosed, even though the information is legitimate.[9]

Different privacy norms may exist in varied areas of life. For example, a person may be willing to reveal information to a doctor or psychologist that she would not share with her spouse or friends. Individuals have the ability to choose how their personal information is collected, used,

[5] Jerry Kang, *'Information Privacy in Cyberspace Transactions'*, 50 Stanford Law Review 1193, 1202-03 (April 1998).
[6] Maria Tzanou, *'Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right,'* 3 (2) International Data Privacy Law 88 (1 May 2013)
[7] Strutner v Dispatch Printing Co., 2 Ohio App. 3d 377 (Ohio Ct. App., Franklin County 1982).
[8] Stanley I. Benn, *'Privacy, Freedom, and Respect for Persons,' in 'Nomos XIII: Privacy'*, 26 (J. Ronald Pennock and J.W. Chapman eds., 1971).
[9] Jeffrey Rosen, *'The Unwanted Gaze: The Destruction of Privacy in America'* (Random House, 2000).

and released under data protection and privacy rules. This is because individuals are most qualified to understand how their personal information will benefit or hurt them in the various situations in which it is used.[10]

The right to privacy is not a brand-new concept. It's a common law principle, and an invasion of privacy gives the victim the right to sue for tort damages. ***Semayne's Case (1604)***[11] was one of the first cases on right to privacy. **Sir Edward Coke** famously stated, while acknowledging a man's right to privacy, *"the house of everyone is to him as his castle and fortress, as well for his defense against injury and violence, as for his repose"*. In the 19th century, the concept of privacy was further developed in England, and it is now firmly established around the world. In case of ***Campbell v. MGN[12]***, the court held that *"If an intrusion occurs in a circumstance where a person can reasonably expect his privacy to be respected, the intrusion will be unlawful unless it is justified."*

**RIGHT TO PRIVACY: INDIAN JURISPRUDENCE**

In the case of ***M. P. Sharma and Ors. v Satish Chandra, District Magistrate, Delhi and Ors***[13], the Hon'ble Supreme Court evaluated whether the 'right to privacy' is a fundamental right and the search and seizure warrant granted pursuant to sections 94 and 96(1) of the Code of Criminal procedure[14] was contested. The Hon'ble Supreme Court held that no constitutional provision was infringed by the power of search and seizure. In addition, the Hon'ble Supreme Court did not recognise the right to privacy as a fundamental right enshrined in the Indian Constitution.

Then the matter was considered by the Hon'ble Supreme Court in ***Kharak Singh v State of Uttar Pradesh and Ors.***[15] That whether the surveillance by domiciliary visits at night against an accused would be a misuse of the right enshrined in Article 21 of the Constitution, raising the question whether Article 21 should also include the privacy. According to the Supreme Court, such surveillance was in fact in violation of Article 21. The majority judges went on to say that because Article 21 does not explicitly have a privacy provision, the right to privacy cannot be considered a fundamental right.

[10] Helen Nissenbaum, *'Privacy as Contextual Integrity'*, 79 Washington Law Review 119 (2004).
[11] Peter Semayne v Richard Gresham, 77 ER 194.
[12] Campbell v. MGN, 2004 UKHL 22.
[13] M. P. Sharma and Ors. v Satish Chandra, District Magistrate, Delhi and Ors, 1954 SCR 1077
[14] The Code of Criminal Procedure, 1973, (Act No. 2 of 1974).
[15] Kharak Singh v State of Uttar Pradesh and Ors., (1964) 1 SCR 334.

Thereafter, in the case of ***Gobind v State of M.P.***[16], the police's power to conduct domiciliary surveillance was challenged as being incompatible with the right to privacy guaranteed by Article 21 of the Indian Constitution. The Supreme Court held that the police regulations were in violation of the essence of personal liberty, and while it recognised the right to privacy as a fundamental right guaranteed by the Indian Constitution, it favoured the evolution of the right to privacy on a case-by-case basis rather than treating it as absolute.

Following that, in ***People's Union for Civil Liberties (PUCL) v Union of India***[17], the Hon'ble Supreme Court stated unequivocally that the right to privacy is guaranteed in Article 21 of the Constitution as part of the right to "*life*" and "*personal liberty*." When the facts of a case give rise to a right to privacy, Article 21 is invoked. The said right cannot be reduced "*except according to procedure established by law*".

This issue was recently raised before the Hon'ble Supreme Court in the case of ***K. S. Puttaswamy (Retd.) v Union of India***[18], in which the 'Aadhaar Card Scheme' was challenged on the grounds that collecting and compiling demographic and biometric data of the country's residents being used for multiple purposes is in violation of the fundamental right to privacy embodied in Article 21 guaranteed by the Indian Constitution. The Hon'ble Supreme Court referred the case to a constitutional bench consisting of 9 judges due to ambiguity in past judicial judgments on the constitutional status of the right to privacy and held that the right to privacy is essential to and inseparable from the human element in a human person, as well as the core of human dignity. As a result, it was determined that privacy had both positive and negative implications. The negative element prevents the state from infringing on a citizen's life and personal liberty, while the positive content requires the state to take all reasonable steps to protect the individual's privacy. The right to privacy has now become *"stronger than a mere common law right"* and *"more robust and sacred"* than any statutory right as a result of this decision. Under Article 21 of the Constitution, an invasion of privacy must now be justified by "a law" that specifies a fair, just, and reasonable approach.[19]

The Hon'ble ***Mr. Justice D.Y. Chandrachud***[20] concluded as follows while analysing the right

[16] Gobind v State of M.P., (1994) 6 SCC 632.
[17] People's Union for Civil Liberties (PUCL) v Union of India, (1997) 1 SCC 301.
[18] K. S. Puttaswamy (Retd.) v Union of India, (2015) 8 SCC 735.
[19] *"Data-Protection-26-Privacy-Issues-in-India.Pdf,"* accessed August 25, 2021, https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf.
[20] Hon'ble Mr. Justice D.Y. Chandrachud wrote the judgment on his own behalf and on behalf of Hon'ble Mr. Justices J.S. Khehar, R.K. Agrawal & S. Abdul Nazeer

to information privacy in present era: The right to privacy includes informational privacy as well. Regarding the perils of privacy in the digital era, non-state actors can also provide information. He also commended Union Government to investigate and implement a strong data protection regime.[21] He further stated that *"The right to privacy is claimed qua the State and non-State actors. Recognition and enforcement of claims qua non-state actors may require legislative intervention by the State."*[22]

## DATA PROTECTION : EVOLUTION OF DATA PROTECTION STATUTES IN INDIA

India has been swept up in the digital revolution that is engulfing the world in this technological age. Recognizing its importance and the potential for significant disruption in practically every facet of society, India's government devised and implemented the **"Digital India"** plan.[23] India is well on the road to becoming a digital economy, with about 450 million Internet users and a growth rate of 7-8 percent, and a significant market for foreign firms.[24]

India has seen a number of cases of data theft that have been averted by cyber security teams. As a result, an effective and well-formulated process is essential to prevent data theft. India's current data protection rules are limited in scope. In the lack of statutory provision, the provisions of the Information Technology Act, 2000, as amended by the **Information Technology (Amendment) Act, 2008**[25], have been used to secure data in India. This act, however, is neither data nor privacy protection legislation in the conventional sense. It is a generic piece of legislation that has no specific data protection or privacy standards.[26]

**The Copyright Act of 1957** [27]can also be used to safeguard personal information. It provides some opportunity for safeguarding different sorts of data as literary works because it protects intellectual property rights in various types of creative works, including literary works. Furthermore, the **Indian Penal Code 1860** may be used to deter data theft.

---

[21] Daniel Solove, *'10 Reasons Why Privacy Matters'* published on January 20, 2014 https://www.teachprivacy.com/10-reasons-privacy-matters/.
[22] Justice K S Puttaswamy, "IN THE SUPREME COURT OF INDIA CIVIL ORIGINAL JURISDICTION," n.d., 547.
[23] *"MeitY_TrillionDollarDigitalEconomy.Pdf,"* accessed August 29, 2021, https://www.digitalindia.gov.in/ebook/MeitY_TrillionDollarDigitalEconomy.pdf.
[24] Ibid.
[25] "Information Technology Act, 2000," 21 of 2000 § (2000), https://eprocure.gov.in/cppp/staterulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=.
[26] *"Does India Have a Data Protection Law?,"* accessed August 29, 2021, https://www.legalserviceindia.com/article/l406-Does-India-have-a-Data-Protection-law.html.
[27] The Copyright Act of 1957, (Act no. 14 of 1957).

The Indian Ministry of Communications and Technology announced four sets of rules implementing key features of the act, the first of which is pertinent to the subject of data protection, in April 2011, following the European Union implemented rigorous and stringent Data Protection laws. This list of regulations also includes the **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (2011)**[28], which were enacted under Section 43A of the IT Act. Section 43A states that if a body corporate possesses, deals with, or handles any sensitive personal data or information in a computer resource that it owns, controls, or operates is negligent in implementing and maintaining reasonable security practices and procedures, and thereby causes wrongful loss or gain to any person, the body corporate will be liable to pay damages as compensation.

Except for IT rules, no statute defines personal data. Furthermore, the IT Rules require the Body Corporate to create a privacy policy, which must be available on the Body Corporate's website.[29] The policy should cover personal information and sensitive data, including the reasons for collecting it and how it will be used. The IT Rules also cover the process and procedure that the Body Corporate should follow while collecting personal information and sensitive data. It further stipulates that the Body Corporate cannot keep the information for any longer than is necessary by law. As a result, the new regulation is harsher and more rigid, and it is in line with EU standards and the Body Corporate must comply with IT rules and maintain openness in its new privacy policies.

However, the existing mechanism falls short in the area of data protection because the statutes in question were not written especially with data protection in mind, and the current legislation contains numerous loopholes in terms of effective data protection. The government introduced the Privacy Bill in 2011 to address this issue, but it has yet to become legislation.

## EXISTING REGULATORY ISSUES RELATING TO DATA PROTECTION

1. As enumerated by the Hon'ble Supreme Court in ***K. S. Puttaswamy (Retd.) v Union of India***[30]***,*** there is a need for a threefold requirement for State's interference with the

[28] Supratim Chakraborty, *"Data Protection in India: Overview," A w*, 2021, 22.
[29] "IT(Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 English.Pdf," accessed August 29, 2021, https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf.
[30] Ibid 21.

fundamental rights : Though the State may take action to preserve the legitimate interests of the State,

(a) A law must be in place to justify the violation of privacy, as expressly provided for in Article 21 of the Constitution,
(b) The type and substance of the law imposing a limitation must fall within the reasonability zone stipulated under Article 14; and
(c) The means used by the legislature shall be proportionate to the purpose and the needs to be met by law.

Consequently, any law that seeks to infringe a person's right to privacy would need to meet the *'test of proportionality and reasonableness'*.[31]

2. It is widely advocated that India should switch to a **"rights-based"** data protection paradigm rather than the current **"consent-based"** model. Once the user's approval is secured under the consent-based approach, the data controller is free to use, process, and share the data with any third parties. However, few people are aware of the actual ramifications of inadvertent data sharing when they give their approval. The 'rights-based' model, on the other hand, allows users to have more control over their data while also requiring the data controller to ensure that these rights are not violated. As a result, users have more control over their personal data.
3. After recognizing that laws were not implemented with personal data protection in mind, the Indian government has advocated enacting separate privacy legislation. A private member's bill, the **Data (Privacy and Protection) Bill, 2017**[32], was also submitted in parliament, calling for the institution of a Data Privacy and Protection Authority to regulate and adjudicate privacy-related disputes.

As can be seen from the points listed above, a comprehensive law governing the gathering and transmission of personal data is urgently needed. There are no thorough regulations governing the processing of non-sensitive personal data or information.

Following its acquisition by Facebook Inc., WhatsApp Inc. changed its privacy policy, informing users that "WhatsApp" account information would be shared with "Facebook" to improve "Facebook" ads and product experiences, and users were asked to agree to the revised

[31] Ajoy P.B., *"Administrative Action and the Doctrine of Proportionality in India," IOSR Journal of Humanities and Social Science* 1, no. 6 (2012): 16–23, https://doi.org/10.9790/0837-0161623.
[32] Data (Privacy and Protection) Bill, 2017, (Bill No.100 of 2017).

terms by September 25, 2016, in order to continue using WhatsApp.[33] In light of this development, Karmanya Singh Sareen and others filed a writ petition in the Hon'ble High Court of Delhi, claiming that removing the privacy protection of "WhatsApp" users' data and sharing it with Facebook was a violation of the users' fundamental rights guaranteed under Article 21 of the Constitution. The Hon'ble Delhi High Court, in ruling on the case, stated that if users choose to delete their WhatsApp accounts completely, WhatsApp will delete their data from its servers and will not share their data with Facebook, and that users who choose to stay in "WhatsApp" will have their existing information/data/details up to September 25, 2016 preserved. The court also ordered the government to look into whether bringing messaging platforms like WhatsApp under a statutory regulatory framework is viable. However, a special leave petition has been filed before the Hon'ble Supreme Court of India challenging this judgement.[34] The matter is *sub-judice* and awaiting a decision. The Supreme Court's decision and the government's policy will, nevertheless, have a significant impact on how personal data is managed in India, particularly by non-state entities.

In general, India lacks a robust data protection and regulation framework. To secure private data, a strict rule addressing all aspects of data protection and encompassing requirements of all the scattered legislations must be implemented. The government should *"put in place a robust regime for data protection"* in light of the growing threat to privacy from both state and non-state actors.[35] Furthermore, the IT Act, the Right to Information Act, the Right to Privacy Act, the Aadhaar Act and the rules enacted statutorily, as well as additional regulations governing sectors such as telecom, banking, medicine and healthcare, and insurance, may all directly or indirectly govern the privacy and data protection domain in India.

## WHETHER EXISTING SYSTEM IS ADEQUATE?

In order to correctly adopt and execute legislation on the protection of private data, it is impertinent to identify the shortcomings after a critical review of literature. There can be no denying the need for a special law. However, further questions need to be asked regarding accessibility concerns, who accesses personal information, and to what extent?, the subject of accountability, the development of a data protection authority, the issue of adjudication of data violation cases and other regulatory issues. These issues shall be discussed with special

[33] Karmanya Singh Sareen v UOI, 2016 SCC Online Del 5334.
[34] Karmanya Singh Sareen v. Union of India, SLP (Civil) No. 804/2017.
[35] Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., Writ Petition (Civil) No. 494 of 2012.

reference to The Personal Data Protection Bill, 2018.

## THE PERSONAL DATA PROTECTION BILL, 2018

The 2018 Personal Data Protection Bill provides India with broad data protection protections to its residents. It was formulated on 27 July by a committee led by former Supreme Court Judge B N Srikrishna. It sets the context for Indian data protection legislation and describes how an organisation is supposed to acquire, handle and store data for citizens. The objective of Personal Data Protection, 2018 is to *"ensure growth of the digital economy while keeping personal data of citizens secure and protected."*

This bill is applicable to public as well as private entities. Any person who processes personal data in connection with any business in India, systematic offer of goods and services to the data principals in India or activity involving the profiling of personal data directors within Indian Territory will have the law's application, if it performs data controllers or data processors not present within the territory of India. It asserts privacy as a fundamental right and requires personal data to be protected as an integral component of information confidentiality. One of the most significant ideas in the Committee's White Paper was to establish a high-powered authority with regulatory capabilities. There are two models that are also mentioned, the European Union's model, which tends towards privacy of individuals and the US and gives innovations prominence over regulation.[36] It states that personal data can only be processed on the basis of :

- Consent of the owner;
- If being utilised for the working of the state;
- If authorized by law or needed for compliance of a judicial order;
- If necessary for an emergency;
- For employment purposes;
- For reasonable purposes as notified by the data protection authority.[37]

The bill places an excessive amount of power in the hands of the central government, particularly under Section 98, which states that the central government not only has the

[36] *"What India Needs: Data Law, Regulator," The Indian Express* (blog), June 26, 2018, https://indianexpress.com/article/india/what-india-needs-data-law-regulator-5118806/.

[37] *"Regulatory measures of Data Protection in India: Need of the hour",* International Journal of Science & Engineering Development Research (www.ijsdr.org), ISSN:2455-2631, Vol.4, Issue 5, page no.75 - 78, May-2019, Available :http://www.ijsdr.org/papers/IJSDR1905012.pdf

authority to issue directions to the authority, but also that the authority is bound by those directions on policy questions where the central government's decision is final.[38] Furthermore, the bill's criminal liabilities, which make all offences cognizable and non-bailable, are concerning.

## THE PERSONAL DATA PROTECTION BILL, 2018: CHALLENGES AND NEED OF THE HOUR

The Personal Data Protection, 2018 is criticized for being unclear about critical topics. The Organizations will however have to guarantee that they manage personal data wisely when the bill comes into effect. Conditional notices, consents and procedures will oblige organisations to rebuild their key systems, to seek fresh consent and to change their data practises that will ultimately increase the costs of compliance for corporations.[39] There are significant limitations, but the Private Data Protection Bill 2018 is a step forward and should be encouraged to act after its speculation. An independent Data Protection Authority with a normative framework needs to be established and empowered to ensure that data privacy issues are effectively assessed and disseminated. It should be sufficiently competent to handle and issue binding orders in cases of disagreement. The prescription of rules and processes may constitute a quasi-legislative body. It could contain know-how personnel, professionals and skilled people supported by local and central police intelligence services in order to provide rapid remedies.

Furthermore, data controllers and processors should take particular procedures based on norms and legislation with defined liability in the event of a data breach in terms of accountability and integrity. To establish greater accountability, data protection standards should be implemented, with a supervisory authority demonstrating such implementation if necessary. A method for detecting and preventing data breaches should also be put in operation. Because data breach concerns issues of privacy, which is a fundamental right under Article 21 of the Indian Constitution[40], it is vital to take preventative steps.

It's been a year since the Indian government tabled the Personal Data Protection Bill, 2019, in Parliament, but there's still a lot of uncertainty about the final draft of the legislation's enactment and implementation. The Indian data protection standards remain a legal

[38] *"Justice Srikrishna's Data Protection Bill for India Is Full of Holes — Quartz India,"* accessed September 1, 2021, https://qz.com/india/1343154/justice-srikrishnas-data-protection-bill-for-india-is-full-of-holes/.
[39] *"PERSONAL DATA PROTECTION LAW IN INDIA – Legal Developments,"* accessed September 1, 2021, https://www.legal500.com/developments/thought-leadership/personal-data-protection-law-in-india/.
[40] India Const. Art. 21.

conundrum, and the law appears to be mired in legislative procedure and formality, with the law currently in the last phases of parliamentary scrutiny - being assessed by a Joint Parliamentary Committee. In December 2020, a government member of the Joint Parliamentary Committee claimed that the Personal Data Protection Law would not be enacted in its current form, and that *"the bill in itself is not something that is working....And that the committee is...going to redraw the bill."*[41]

## CONCLUSION

Given the expansion and ramifications of international trade, particularly in light of the Internet's influence, it is critical that India work with the international community to adopt rigorous privacy and personal data protection regulations. Currently, countries (such as the EU) are reluctant to trade with India due to inadequate privacy legislation. This is especially important as India becomes a hotspot for back-office operations such as credit processing, medical transcription, and so on. The threat of privacy is also a barrier to establishing a secure environment for Internet communication. Unless these difficulties are addressed, India will be unable to fully profit from the enormous prospects and benefits that e-commerce offers to developing countries like ours.

The absence of a data protection regulation is also a major setback for India's outsourcing business. India might move much further beyond being a mere service provider to the world's major enterprises by enacting a strong data privacy law. Whatever steps the government can take now in light of the situation, it should do so, and the rest will follow. The process is slow, but it can be accomplished if the authorities take it under consideration in parliamentary proceedings. The 2018 Private Data Protection Bill is a good start toward a desired goal. With the enactment of the Bill, the Judiciary will also be well equipped on deciding on matters pertaining to data protection and right to privacy in justice, equity and good conscience. *'The report is like getting new shoes,'* **Justice Srikrishna** said eloquently in reference to the law. *"It'll feel snug at first, but with time, it'll grow more comfortable. It will be interesting to watch whether Indians become accustomed to these shoes or return them."*

[41] "*Data Protection Bill Won't Get Cleared in Its Current Version — BJP MP Rajeev Chandrasekhar – ThePrint,"* accessed September 1, 2021, https://theprint.in/india/data-protection-bill-wont-get-cleared-in-its-current-version-bjp-mp-rajeev-chandrasekhar/568003/.