INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

Volume 3 | Issue 5 Art. 4

2024

Data Protection Bill 2023: The Great Firewall of Privacy Illusions

Kashish Jain

Recommended Citation
Pratishtha Sharma, *Data Protection Bill 2023: The Great Firewall of Privacy Illusions*, 3 IJHRLR 103-126 (2024).
Available at www.humanrightlawreview.in/archives/.

Data Protection Bill 2023: The Great Firewall of Privacy Illusions

Kashish Jain

LLM Student, Jindal Global Law School, O.P. Jindal Global University, Sonipat

Manuscript Received	Manuscript Accepted	Manuscript Published
06 Sept. 2024	10 Sept. 2024	16 Sept. 2024

1. WELCOME TO THE PRIVACY CIRCUS: AN OVERVIEW

The right to privacy is an inherent and fundamental right that is universally acknowledged and should be safeguarded by all nations. In recent times, States have been hesitant to prioritize the threat posed by the acquisition of citizens' personal data, particularly with the increasing risk to user privacy from the Internet of Things (IoTs).

The right to privacy is an innate fundamental right which is globally recognised and must be protected by all states. Over the years, States have been reluctant to pay maximum attention to the threat posed by the acquisition of citizen's personal data until recent times, especially with the growing threat posed by the IOTs to the privacy of users.

With the advancement of the Internet, massive amounts of personal data pertaining to individuals, employees and customers are being transmitted across countries globally. Also, as many international corporations have customer databases and warehousing facilities in different international locations, such data transfers frequently occur between and among units Personal data has become essential resources for the global economy. As a result, the security of data and privacy has become a significant concern for individuals. Confidence in data processing and privacy protection is now necessary for the

successful adoption of electronic commerce within the same corporate enterprise that are situated in different countries. Personal data are now crucial raw materials of the global economy; data protection and privacy have emerged as issues of concern for individuals; and confidence in data processing and privacy protection have become important factors to enable the acceptance of electronic commerce.[1]

Facilitating the movement of data across international boundaries is essential for obtaining essential digital services. In order to remain competitive in international marketplaces, firms must have the capability to transfer not only physical goods, human resources, and knowledge, but also digital data to foster creativity. The presence of rules that facilitate the transmission of data across borders will have a substantial impact on promoting research, technological advancement, and economic growth. Data Protection and privacy legislations often regulate the movement of personal data across national borders; which such movement may be designed by a variety of terms, it will be referred to herein as 'transborder data flows', since this is a term used in the OECD Guidelines.Despite the importance of transfers, many governments still seem oblivious to their social and economic impact. Indeed, transborder data flows have often been considered to be a 'niche' subject of interest only to Data Protection and privacy specialists.

Cross-border data flows add value to not only to services and e-commerce industries, but also to manufacturing. A study by McKinsey Global Institute in 2011 found that 75% of the value added by the Internet goes to the traditional manufacturing

[1] Kuner, C. (2010) 'Regulation of Transborder Data Flows under Data Protection and Privacy Laws: Past, Present and Future', *Tilberg University Legal Studies Working Paper No. 016/2010* [Preprint].

sector.[2]Another study by the McKinsey Global Institute in 2016 estimated that all forms of global flows (such as goods, services and capital flows) increased global GDP by at least 10% (which amounted to USD 7.8 trillion), of which Internet Data flows made up USD2.8 trillion.[3] These figures highlight the broad economic potential of the Internet data flows made up USD 2.8 trillion.[4] These figures highlight the broad economic potential of the Internet as a business platform for many aspects of international trade and foreign investment.[5]

Although international data transfer assists both businesses and consumers, while generating benefits for the economy at large, several countries (both developing and developed) have imposed heavy restrictions on cross-border transfer of data. These proffered justifications for such restrictions include policy concerns like safeguarding privacy and security, but digital protectionism may also be at play,[6] entailing for example the promotion of the local information and communication technology industry either directly by providing preferential treatment in government procurement to domestic cloud computing companies, or indirectly by coercing foreign companies to locate their servers domestically. These restrictions tend to reduce market access for foreign suppliers of digital services, impeding

[2] Matthieu Pelissie Du Rausas, Supporting the Internet as a Platform for International Trade 1 (2014); Joshau P Meltzer, The Internet, Cross Border Data Flows and International Trade, 2 Asia and the Pacific Poly Studies 90, 92 (2014)
[3] James Manikya & Susan Lund, Dhruv Dhingra, Digital Globalization: The New Era of Global Flows 1 (2016).
[4] James Manika, Susan Lund, Jaques Baughin, Jonathan Woetzel, Kalin Stamenov and Dhruv Dhingra, Digital Globalisation and the New Era of Global Flows 1 (2016)
[5] Joshau P Meltzer, Supporting the Internet as a Platform for International Trade 1 (2014)
[6] Azmeh, S. and Foster, C. (no date) 'The TPP and Digital Trade Agenda: Digital Industrial Policy and Silicon Valley's influence on new trade agreements', *LSE International Development, Working Paper No 16-175, 2016*, 11.

trade and investment opportunities and increasing the costs and service choice of individual businesses.[7]

The Digital Personal Data Protection Act, 2023 (hereinafter referred to as 'the Act) was passed by both houses of the Indian Parliament and has received Presidential Assent. One of the key considerations of the Act is its impact on Cross Border Data Transfers.[8] While the Act is yet to come into force, and the rules will prescribe further clarity on the implementational aspects are awaited, it becomes our burden to assess the potential impact on cross-border transfers of personal data under the new regime.

2. FROM FREE DATA FLOW TO DIGITAL BORDERS: A HISTORICAL GAG REEL

Historically, the Europeans have long valued data protection-specifically, protection of the citizen against abuse of his or her data and protection of privacy. Data protection and privacy law in the European Union is largely a reaction to the Nazi Party's creation of a total surveillance state from 1933-1945.

The First Data Protection law is generally considered to be that of the German federal state of Hesen, which was adopted in 1970 and did not contain any restriction on the transborder data flows.[9] Shortly after this, many European countries enacted data protection laws containing restrictions on transborder dataflows.[10] Examples of these include laws of Austria, Finland,

[7] 'Cross-border Data Flows: Could Foreign Protectionism Hust US Jobs? Hearing before Sub-Comm on Commerce, Mfg, and Trade of the Comm on Energy and Commerce, ' (no date) *113th Cong, 8 (2015)* [Preprint], (H of Rep).
[8] V Rajesh & H Tavawalla, *India: Digital Personal Data Protection Act, 2023-what it means for cross-border transfers,* November 2023,
[9] Hessisches Datenschutzgestz, 7 October, 1970
[10] Brothe, M. and Killian, W. (no date) *Rechtsfragen Grenzuberschreitender Datenflusse (Verlag Dr. Otto Schmidt)*, pp. 529–565.

[11] France, Ireland, [12] Luxemborug and Sweden.[13]

The restrictions contained in these early laws range from a requirement to obtain an explicit authorization from the data protection authority before transferring personal data outside the country (e.g. in Australian and Swedish Law); to adopting verbatim the provisions of Art 12 of the Counsel of Europe Convention 108 (as in the case of Irish Law); to a requirement that either the individual whose data was transferred had to consent to the transfer, or that country of import had to have data protection law with a similar level of protection (as in the case of Finnish Law). However, despite these provisions, at the time the first data protection laws were drafted the transborder flow of personal data seems to have been regarded as the exception instead of the rule.[14]

The OECD Privacy Guidelines represent the first attempt to deal with transborder data flows from a global perspective. Adopted in 1980, the Guidelines are a non-binding set of principles that member countries may enact, and have the dual aim of achieving acceptance of certain minimum standards of privacy and personal data protection, and of eliminating, as far as possible, factors which might induce countries to restrict transborder data flows for reasons associated with such flaws.[15]

In 1990, the United Nations issued its Guidelines concerning Computerized Personal Files, which take the form of a non-binding guidance document.[16] The UN General Assembly

[11] Personal Data File Act & Personal Data File Decree, 30 April 1987, 22
[12] Data Protection Bill, 1987, superseded by the Data Protection Act, 1998.
[13] Swedish Data Act of 1973, Art 11
[14] F. Hondius, International Data Protection Action, Policy Issues in Data Protection and Privacy, (n 6) at 208
[15] OECD Guidelines, Explanatory Memorandum, para 25
[16] UN Guidelines concerning Computerized Personal Data Files of 14 December 1990

requested 'governmental, intergovernmental and non-governmental organisations to respect those guidelines in carrying out the activities within their filed of competence.[17] Regulation of transborder data flows may restrict the provision of services across borders, which may give rise to questions under the General Agreement on Trade in Services (GATS), a treaty of the World Trade Organisations (WTO) that entered into force in 1995.[18] Data protection Regulation (including regulation of transborder data flows) is exempted from scrutiny under the GATS, but only as long as it does not represent a disguised restriction on trade.[19]

In 1981 the Council o Europe enacted its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (referred to here as 'Convention 108')[20] The Convention, which has been called 'the hereto sole international treaty dealing specifically with data protection', entered into force on 1st October 1985, and at this time this study was finalized has been ratified and acceded to by 42 countries (mainly in Europe). Significantly, the Convention is open also for signature by countries that are not member states of the Council of Europe, though no non-member has so far enacted it.

In 2001, the Council of Europe adopted an Additional Protocol to the Convention, which provides that each party shall allow the transfer of personal data to a non-party only if an 'adequate level of data protection' is assured (Article 2(1) of the Additional Protocol). However, by ay of derogation, such transfers are also

[17] UN Guidelines concerning Computerized Personal Data Files of 14 December 1990
[18] Peter P Swire, Robert E Litan, None of Your Business: World Data Flows, Electronic, Commerce, and the European Privacy Directive, Brookings Institution Press, 1998, 189-196
[19] GATS Article XIV(c)(ii)
[20] January 28, 1981, ETS 108 (1981)

allowed if 'domestic law provides for it because of specific interests of the data subject or legitimate prevailing interests, especially important public interests' (Art 2(2)(a)), or 'if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law' Art 2(2)(b).

Perhaps the most influential legal instrument regulating transborder data flows I the EU Data Protection Directive 95/46 (the 'Directive').[21] Adoption of the Directive was spurred by cases in which the free flow of data between the Member States of the European Communities was threatened by the varying levels of data protection applicable in them.

In 2004, the twenty-one member economies of the Asia-Pacific Economic Cooperation (APEC) group agreed on the APEC Privacy Framework, which is a set of privacy principles that member economies may implement voluntarily. The Framework protects the personal data transferred outside the APEC member states where they were collected by recourse to the principle of 'accountability'.[22]

3. A NOT-SO-GLOBAL VILLAGE: UNDERSTANDING CROSS-BORDER DATA TRANSFERS

Before examining the Data Protection Act of 2023, and its tackling of cross-border data transfer and flows of personal data it is necessary to analyse the traditional legal challenges that come

[21] Directive EC 95/46 of the European Parliament and of the Council of 24th October 1995 ON THE Protection of individuals with regard to processing of personal data and on the free movement of such data.
[22] APEC Privacy Framework (n2), Principle 9

with transaction with Cross-Border Personal Data transmission.[23]

- ***Jurisdiction Challenge***

Many 'Cloud Providers' when it comes to context of cloud computing services are based overseas. Subsequently, the clauses in relation to the location of data perform an important role in determining the jurisdiction, as well as the level of data and privacy protections cloud users are afforded. Traditionally, it is relatively easy to find the location of web servers, and data is stored in the data centres of the web service providers. In a cloud environment, many cloud providers are using virtual servers to provide data servers to provide data storage and process services. It is somewhat a challenge to identify where the data storage is located.[24] In addition, both the primary location of the data and any backup locations determine which countries' laws and regulations must be followed.

In Cloud computing related disputes, the jurisdictional issues are always complex. Cloud service contracts have been responsible for intensifying many potential jurisdictional challenges.[25] Cloud service contracts often include a jurisdiction provision that specifies the governing legislation of the contract. Contracts that include jurisdictional clauses diverting the relevant law from the user's domicile may lead to a restricted ability to enforce the contract. Therefore, it is important for both cloud providers and customers to pay close attention to Service Level Agreements (SLAs). Cloud providers

[23] George Yijun Tian, Current Issues of Cross-Border Personal Data Protection in the Context of Cloud Computing and Trans-Pacific Partnership Agreement: Join or Withdraw, 34 WIS, INT'ILJ 367 (2016)
[24] Paul M Schwartz, EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation, 12 BNA PRIVACY and SECURITY L REP, 718, 718 (2013)
[25] Trans-Pacific Partnership Agreement, AUSTI. GOVT DEPT of FOREIGN AFF & TRADE ch 14, October 6, 2015.

and consumers must give careful consideration to the 'jurisdiction clause' and the 'data location clause' specified in SLAs. Merely having a well-crafted Service Level Agreement (SLA) and a jurisdiction clause does not guarantee that cloud users and providers will be completely immune to jurisdictional disputes.

- ***Privacy and Security Challenges***

Ensuring data security is a big worry for businesses and individuals contemplating a transition to the Cloud. There are several privacy and security risks associated with protecting personal data in the cloud, especially when it comes to cross-border data protection. These entail:

The Challenge of Legal Compliance

Data transmitted over the internet will traverse international boundaries, necessitating data owners, cloud service providers, and data consumers to address the privacy and security risks inherent in cross-border data transmission, as well as comply with legal requirements pertaining to such transfers.[26] The worldwide character of data transfer, in contrast with the constraints of national legislation, has resulted in a fragmented legal framework that applies domestically, despite the fact that data storage and transfer occur globally. Therefore, when cloud service providers establish data storage centers, they must be cognizant of and adhere to the laws of the country where their data storage centers are situated, especially those pertaining to the movement of data across borders, in order to avoid legal consequences. Similarly, when individuals select their cloud

[26] Peter K Yu, Towards the Seamless Global distribution of Cloud Content, in PRIVACY and LEGAL ISSUES IN CLOUD COMPUTING, 180-181

service providers, they should have a thorough understanding of the geographical location of the data storage infrastructure used by the provider. This is important because there is a possibility that their personal data may not be adequately protected by the legal regulations of the user's country, leading to a mistaken belief of privacy.

Security Challenges with outsourcing arrangements

The subcontracting and outsourcing arrangements that involve foreign companies also present extra risks for both cloud service providers and users. These include:

- Risks for sub-contractor businesses who must navigate with their relevant legal obligations in protecting personal data under foreign laws; and
- Privacy and security risks for the user who is perhaps unaware of the commercial or political arrangements relating to their personal data and the subsequent application of foreign laws.

Although the cloud provider market is expanding, there are still only a limited number of large companies that have the capacity to offer large-scale application and data hosting independently.

- ***Convergence Challenges***

Convergence challenges for cross-border personal data protection are two-fold:

Challenges From Convergence of Technology

Digital convergence can be used to explain the evolution of technology services and industry; however, the term has been

further developed by Collins[27] and Gates[28] to describe the 'coming together of telecommunications, computing and broadcasting into a single digital bit stream'[29]. Digital Convergence presents both opportunities and risks; it has significantly promoted innovation, efficiency, and contributed to public enjoyment of new technology. It also poses a challenge, however, for traditional models of commercialising and protecting personal information (personal data), including cross-border personal data.[30]

Challenges from Convergence of Law

It has become increasingly evident that the 'convergence of technology' has intensified the 'convergence of law' across different sectors of law. The Internet is borderless in nature and when goods or service providers put their products or services (including intangible products, such as gaming software) on the Internet, they are trading with customers worldwide rather than a single national market. As a consequence, the laws in foreign countries may extent the jurisdictions hey are subject to.

The fact remains that the existing Rules of International Trade do not protect cross-border data transfer in a consistent, coherent and predictable manner and there are lessons to be learnt here, when it comes to the implementation of our very

[27] Richard Collins, Back to the Future: Digital Television and Convergence in the United Kingdom, 22 TELECOMM POL'Y 383, 385 (1998)
[28] Arlan Gates, Convergence and Competition: Technological Change, Industry Concentration, and Competition Policy in the Telecommunications Sector, 58 U of TORONTO FAC of L REV 83 (2000)
[29] Martha Garcia-Murillo & Ian Macinnes, The Impact of Technological Convergence on the Regulation of ICT Industries, 5 INT'LJ on MEDIA MGMT. 57,57 (2002)
[30] Paul T. Jaeger et al, Where is the Cloud? Geography, Economics, Environment and Jurisdiction in Cloud Computing, 14 FIRST MONDAY (May 4, 2009)

own Data Protection laws.[31]

4. MEET THE STAR OF THE SHOW: DATA PROTECTION BILL 2023

The DPDPA was initially borne out of a landmark Supreme Court ruling that established a constitutional right to privacy, *Justice K.S. Puttaswamy v. UOI,*[32] a development which began in the year 2012 when the Justice petitioned against linking state benefits to a mandatory universal identification card called the Aadhaar. The Court issued a unanimous verdict affirming that privacy is a right protected by the constitution. This verdict carries substantial ramifications for numerous matters throughout Indian society. As an illustration, it played a substantial role in establishing the legal foundation for a groundbreaking judgment in 2018 that removed criminal penalties for consenting sexual activity between individuals of the same gender, which was previously prohibited under Section 377. Furthermore, in the context of the Puttaswamy verdict, the government established an expert group led by Justice B.N Srikrishna with the purpose of providing recommendations for data legislation. In 2018, the committee presented its findings and a preliminary version of the bill to the Ministry of Electronics and Information Technology (MietY). Subsequently, in 2019, the Ministry proposed the first version of the Data Protection and Privacy Bill (DPDPA) to Parliament. Subsequently, the bill that ultimately transformed into the DPDPA has undergone significant changes.

According to the Act, it is allowed to transfer personal data across borders. Nevertheless, Section 16(1) of the Act empowers the

[31] Andrew D Mitchell, Jarrod Hepburn, Don't Fence Me In: Reforming Trade and Investment Law to Better facilitate Cross-Border Data Transfer, 19 YALE J.L & Tech, 182 (2017)
[32] *Justice K.S. Puttaswamy v. UOI*, (2017) 10 SCC 1

Government to limit the transfer of personal data to specific countries or territories outside India through a notification. The existing version of the Act does not offer more elucidation regarding the nature of the restrictions. These limits may involve imposing additional requirements, similar to the adequacy tests used in the GDPR, for transferring personal data to specific countries. The purpose is to limit the transfer of certain types of data. Alternatively, the Government has the option to blacklist countries where the transmission of personal data may be forbidden.

In addition, the Act also deals with the concerns regarding potential conflicts with sector-specific legislation regarding the transfer of data. Presently, sector-specific regulators such as the Reserve Bank of India (RBI) and the Securities Exchange Board of India (SEBI) enforce the compulsory storage of certain data related to sectors, namely payments data and securities data, within India. Section 16(2) of the Act states that if there is another law that offers greater protection or imposes stricter limitations on the transfer of personal data outside of India, that law will take precedence over the provisions of the Act.

It is important to mention that the earlier versions of the data law, prior to the enactment of the Act, included a distinction between personal data and special categories, which included sensitive personal data and essential personal data. This distinction was crucial for achieving higher levels of compliance and data accuracy, respectively. Nevertheless, the Act does not establish any specific differentiation, so allowing the Government to determine the importance of data on an individual basis and impose limits accordingly. Moreover, the Act has implemented a jurisdictional approach, which permits limitations on the transfer of any personal data to designated nations.

The Justice Srikrishna Committee Report in India outlined the provisions for the Cross-Border Transfer of personal data and specified the requirements for such transfers. Additionally, it recommended that the data fiduciary must store at least one copy of personal data on a server or data centre situated in India.[33] The Personal Data Protection (PDP) 2019 legislation permitted the movement of personal data across borders. However, it also proposed imposing limitations on the transfer of sensitive personal data outside of India.[34] The JPC Report 2021 did not make any substantial effort to address this issue directly, but it provided explanations stating that the Central Government should not accept the Cross-Border Transfer of personal data if the purpose of such transfer goes against public policy or government policy.[35] The proposed DPDPB 2022 does not explicitly guarantee the unrestricted transfer of personal data across borders. Instead, it empowers the Central Government to notify the countries or territories outside India to which a Data Fiduciary may transfer personal data, based on the subjective satisfaction of the Central Government.[36]

5. THE TUG-OF-WAR: PRIVACY TAKES ON SECURITY

There are multiple articles that have expressed detailed opinions on the fundamental right to privacy. In fact, it can be deemed to be second generation right that has evolved into a third generation right. In dealing with the formal understanding of privacy, Samuel Warren and Louis Brandeis[37] defined privacy as "the right to be let alone." Although, it embraces the essence of privacy,

[33] Justice Shrikrishna Committee Report, Sec 40(1)
[34] Personal Data Protection Bill, 2019, Sec 33(1)
[35] JPC Report, 2021, Recommendation no 52
[36] Digital Personal Data Protection Bill, 2022
[37] Drushti Desai, Hardik Upadhaya, Security and Privacy Consideration for Internet of Things in Smart Home Environment, 10 International Journal of Engineering Research and Development (Nov 2014)

nonetheless the concept in itself has however been extended over time to include the protection of one's private domain, ones bodily private sphere (e.g., age, behaviour, passwords etc), confidential conversations about me is known to what people." In summary, privacy focuses on protecting the user's personal information, whether it be the person's identity, locations, movements or any other information related to him/her that the person is afraid to share with others.

The ongoing digital disruption is posing a threat to privacy norms worldwide. The progress in cloud computing, social media, and mobile technology is profoundly transforming the personal and professional lives of individuals throughout the world. The dynamic nature of the interconnected world necessitates law enforcement agencies to periodically strengthen the regime of privacy legislation.

In conclusion, the right to privacy should be seen as an inviolable right, regardless of the level of technological progress and the seeming erosion of these rights due to widespread acceptance. The Right to Privacy is a basic right protected under Article 21 of the Indian Constitution, which is a part of the Right to Life and Liberty. It includes the concept of informational privacy, which refers to the protection of personal data and the control individuals have over their own data.

The debate between privacy and security is to buttress the sanctity of the right to privacy in itself. There has been a lot of debate that the right to privacy should take pre-eminence over security and vice versa. The privacy-security debate profoundly influences how these government activities are regulated, but there is a major problem with these debates: Privacy often looses out to security when it shouldn't. Security interests and readily

understood and give prominence and Privacy remains to be a vaguer, more abstract concept. Protecting Privacy need not to be fatal to security measures, it demands oversight and extensive regulation.

6. CORPORATE JUGGLING ACT: BUSINESS IMPACTS AND COMPLIANCE NIGHTMARES

The prior data protection regime in India only prescribed compliances for the transfer of personal data which is categorized as sensitive personal data or information (passwords, financial information, physical, psychological and mental health conditions and sexual orientation, medical records and history, biometric information).However, given that he Act applies to all kinds of personal data (including name, address, email, phone number, etc), a wider category of personal data, including personal data that may not ordinarily be classified as critical or sensitive, may even be subject to cross-border transfer restrictions. Furthermore, the act itself is designed to have extraterritoriality applicability, i.e. applying to entities outside India. Consequently, foreign companies that collect personal data from individuals in India while offering goods and services are required to comply with the Act. In situations where a country is blacklisted, the transfer of personal data to companies in such a country would not be permissible. It could also be extended to prohibit the primary collection of data by companies located in a blacklisted country. Hence, foreign companies from a blacklisted country may be restricted from directly undertaking business in India (especially online models) as basic personal data would be required for providing goods or services.

It is important to highlight that the Act is not the only set of regulations that govern cross-border transfers. Sectoral

legislation also impose constraints in this regard. Therefore, even if the Government allows the transfer of personal data to a particular nation, if the sector-specific regulation limits or mandates the localization of the data, the transfer would not be allowed. In addition, sector-specific regulators often establish rules on the transfer of sector-specific data, which might encompass both personal and non-personal statistics.

7. CLOWNS, CRITICS AND CHEERLEADERS: STAKEHOLDER CIRCUS

Government and Affiliated Bodies

In India's DPDPA, the broad authority of the central government and data protection agency is especially evident in its ability to modify the regulation in response to suspected incitement against the state. Each draft of the DPDPA has granted exceeding power in order to exempt the most important stakeholder of them all: the government. The Shrikrishna report explicitly asserted that the bill should not distinguish between government and private entities because a citizen's right to privacy is fundamental. The earlier versions of the bill drew from the original Puttaswamy ruling to recommend permitting government exemptions that are 'necessary and proportionate' only in narrow circumstances when there is a legitimate state interest (e.g. national security and violations of the law). However, over its life, the DPDPA was modified to eventually embrace a broad exemption for the central government for a range of reasons, including maintaining public order, preventing incitement, and upholding national security- which is the same list of reasons that are used to justify other exceptional acts of technology policy, such as internet

shutdowns.[38]

Platforms and Businesses

In India's case, the DPDPA allows the central government to identify 2 exception categories of companies:

1. **Categories of liable companies**: Sec 17(3) specifically enumerates 'start-ups' as a category of companies that may be exempt from some or all compliance requirements.

2. **Significant data fiduciaries:** Sec 10(1) also empowers the central government to single out specific companies as Significant data fiduciary. The criteria for identifying these is not fixed or enumerated in law but could possibly encompass volume and sensitivity of personal data processed, risk to user's rights, potential impact to sovereignty and integrity of India, risk to electoral democracy, security of the state, and public order. In prior draft bills, this category was called 'Social media intermediaries' or 'social media platforms', alluding to both the type of companies that may be targeted as significant data fiduciaries and the ways in which the DPDPA has evolved to expand the central government's power to subject specific companies to higher scrutiny.

8. PEEK OVER THE FENCE: HOW OTHERS ARE DOING IT

Data protection in developed countries (such as U.S. and Australia) will be markedly different from that of developing countries (such as China and India).[39] The Unites States

[38] R. Grover, 'Contingent Connectivity: Internet Shutdowns and the Infrastructural Precarity of Digital Citizenship', New Media and Society (2023)
[39] Graham Greenleaf and George Tian, Data Protection Widened by China's Consumer Law Changes, 126 PRIVACY L. & BUS INT'L REP 127 (DEC 2013)

introduced its *Privacy Act* in 1974.[40] In stark contrast China's Personal Information Protection Law is still in the drafting process.[41]

Governments in many countries have regulations to compel cloud service providers to provide government's access to personal data in certain circumstances, such as national security or law enforcement. In such circumstances, it is always difficult for cloud service providers may object, many feel compelled to provide the government access to their customer's personal data, should such a request be made.[42] A quintessential example is the United States *Patriot Act* where multiple recent reports and press articles have expressed grave concerns and regularly asserted the fact that the US Government seemingly has unfettered ability to obtain access to data stored outside of the United States by US cloud service providers or their foreign subsidiaries. There are also concerns that this aforementioned act, allows the US law enforcement and national security agencies unrestricted access to any data, anywhere and at any time.

Like the US, there are other jurisdictions that have comparable legislations that enable their government agencies require access to personal information in the context of national information in the context of national security or law enforcement.

In stark contrast, some regional legal instruments such as the Council of Europe Convention 108,[43] European Convention of Human Rights,[44] and the Charter of Fundamental Rights of the

[40] Privacy Act of 1974, Dept. of Justice
[41] Paul De Hert and Vagelis Papakonstantinou, The Data Protection Regime in China 23 (2015)
[42] Francoise Gilbert, USA Patriot Act Effect on Cloud Computing Services, IT LAW GROUP
[43] Council of Europe Convention 108, Art 1 (ref 'individual's right to privacy, with regard to automatic processing of personal data relating to him.')
[44] European Convention of Human Rights, Art 8 (ref 'Rotaru v. Romania, App

European Union,[45] recognize data protection as a fundamental right, so that the laws regulating the transborder flows of data have the quality of legally binding human rights instruments. There are other instruments that are not particularly based in human right's law and not legally binding. One prominent example is that of the APEC Privacy framework, a rudimentary reading of which will reveal that the terms 'fundamental right' and 'human right' are not used once in the document as it clearly lays more focus on realising the benefits of electronic commerce rather than protecting human rights.[46]

In an attempt to further highlight this contrast, this author would like to point out that in the US, the lack of comprehensive data protection and privacy legislation led to a rushed patchwork of State and Federal laws, making it near impossible for the businesses to comply with all the requirements. Europe, on the other hand, adopted the General Data Protection Regulation (GDPR), which provides a high level of protection for personal data and ensure that Data Flows are consistent across the European Union. In Asia, Data protection and privacy laws vary widely, from comprehensive protection offered by Japan to China's endeavour of cyber-sovereignty by controlling the cross-border transfers of critical data. Thus, there are notable difference between the laissez-faire approach adopted by the EU and the focus on national interests showcased by China.

9. GAZING INTO THE CRYSTAL BALL: THE FUTURE OF DATA PROTECTION IN INDIA

When it comes to our own Data Protection laws, bills and act, this author is of the firm belief that India can only learn from the

No 28341/95, EHCR, 2000-V)
[45] Charter of Fundamental Rights of European Union, Art 8
[46] APEC Privacy Framework (n2) at 3

experiences of these countries as it develops its own approach to cross-border data flows. The Previous DPDPAs contemplates a white list of countries that shall be cleared and notified for cross-border data transfer. The criteria for selecting these countries is yet to be determined/clarified. This, currently, seems to be cumbersome entailing a long list of negotiations with these proposed countries in order to successfully whitelist these countries and automatically blacklisting the countries where negotiations have failed. We are yet to receive extensive clarification on the fact that whether there would be a prohibition on transferring personal data to any other country gets notified or whitelisted by the government. In essence, this approach seems to advocate for imposing a data localisation provision and a non-sharing requirement of digital personal data on the businesses until specific countries are notified as permitted categories.

In order to potentially simplify the complicated issue of cross-border data flows, a suggested solution would be to use the 'Black-List approach' which would involve allowing data to flow freely unless a country is specifically barred or blacklisted. This would allow a seamless flow of Data without trade disruptions or market distortions.

In India, there is also the need to define what 'adequate' data protection and privacy standards. This will ensure that personal data is protected and maintained when it is transferred across borders. The law should also establish clear criteria for determining whether other countries have adequate data protection standards.

The new laws should also allow for the use of Binding Corporate Rules as a mechanism for data transfers. BCRs are rules adopted by multinational companies that provide adequate protection for

personal data across different countries. This will allow for businesses in India to transfer data within multinational groups while still maintaining high data protection and privacy standards.

It s also a suggestion that the law should provide for the use of model contractual clauses as another mechanism for data transfer. These clauses should be standardised and approved by regulatory authorities, and they provide a contractual basis for transferring personal data. This will allow businesses in India to transfer data to other countries while ensuring adequate data protection and privacy standards are maintained.

It has become increasingly clear that India needs to adopt a progressive cross-border data-flow policy that balances privacy and data protection concerns while fostering economic growth. India must look to the experiences of other countries and adopt the best practices to ensure a thriving digital economy that functions to the benefit of all.

10. THE CURTAIN FALLS: WRAPPING UP THE DATA DRAMA

The Indian DPDPA is a broad skeletal framework for a comprehensive data protection regime in India. Much of the guidance on the implementation and enforcement of the Act is anticipated to be introduced by the Government in the form of rules and regulations. It remains to be seen how the broad powers of the Government pertaining to restricting transfers to certain jurisdictions would play out once such notifications are issued under the Act. With the passage of the rules, the applicability of exemptions and practices may also be clarified.

As is clear from the various comparative studied here, it is a

necessity of the hour to restrict the transfer for strategic and national interests should be stuck with legitimate business interests considering that India is an outsourcing hub for many multinational businesses. Stringent restrictions would discourage data-intensive operations from being housed in India.