POLICY PAPER

The Impact of Data Sovereignty on Internet Governance

OONA R. SINGH
ISHA SURI

May 2022

Table of Contents

Executive Summary

Data sovereignty and internet governance have evolved. Interestingly, so have the conceptualisations of them. The internet was previously regarded as hard to govern and regulate due to its bodiless and digital form. This is no longer the case. At the same time, multiple nuanced forms of global internet governance can be simplified into basic approaches.

Models of internet governance can be private-sector led or state-led. We suggest that state-led approaches hold more weight and are the stronger of the two. Additionally, we suggest that multi-stakeholder processes are favourable for policymaking. Multi-stakeholder governance promotes inclusion and collaboration and consensus-approved decision making. These features help develop fair and transparent norms.

An institution often part of public discourse on internet governance is The Internet Corporation for Assigned Names and Numbers (ICANN). ICANN was assigned to manage the internet's Domain Name System (DNS) by the US government. While ICANN's role began primarily in functional capacity, ICANN has become involved in contentious debates over the internet structure. Some argue that ICANN perpetuates a form of American imperialism over the internet. However, ICANN itself claims to employ a collaborative, multi-stakeholder model. As a result, ICANN's role has become heavily politicised. The example of ICANN reflects more significant political dynamics at play in internet governance.

Data has become a precious resource for governments and businesses alike. There is no question whether our data is collected – instead, how it is collected and used is of utmost concern. There should be protection mechanisms in place to ensure data is protected and not misused. Data can be misused and weaponised against individuals and even communities. Thus, there must be frameworks and mechanisms in place that secure and defend citizens' best interests.

Data localisation has become an increasingly popular approach to data and entangled with data sovereignty. Consequently, data localisation is sometimes promoted as a way to exercise data sovereignty. However, data cannot be easily restricted to a single state and localising data cannot be entirely achieved in a state that would like to participate in the global internet. Thus, data localisation is not necessarily a catch-all remedy for states wishing to promote data sovereignty.

There is potential for effective, efficient and fair data governance frameworks in India. Nonetheless, the proposed Non-Personal Data Governance Framework and the Personal Data Protection Bill lack certain areas. Foremost, defining data as simply personal and non-personal is problematic. The provided definition of non-personal data is unsatisfactory, and further classifications of sensitive and non-sensitive data can become harmful. In short, these categories should be revisited. There are also issues with transparency and accountability. The Non-Personal Data Governance Framework was not available for public viewing, and the Personal Data Protection Bill was not available for public commentary. The capacity for harm concerning data should be taken seriously.

In light of the above - we make the following policy recommendations: following the sovereign-difference ideal; focusing on the rights of the individual user; creating a panel of experts to make decisions; promote collaborative policymaking; allow public viewing, discussion, and commentary on policy; provide opportunities for long-term feedback; policies should be sector-specific.

Glossary of Key Term Abbreviations

ICANN – The Internet Corporation for Assigned Names and Numbers

ITU – The International Telecommunication Union

GDPR – General Data Protection Regulation

FTC – Federal Trade Commission

PDB – Personal Data Protection Bill

NPD – Report by the Committee of Experts on Non-Personal Data Governance Framework

DNS – Domain Name System

DSA - European Union's Digital Services Act

EU – European Union

US – United States of America

The Impact of Data Sovereignty on Internet Governance

Oona R. Singh and Isha Suri

1. Internet Governance and Data Sovereignty – An Introduction

Introduction:

The digital landscape has rapidly transformed over the last few decades.

Through this paper, we seek to examine the varying regimes of internet governance globally and provide a helpful framework and suggestions for India. This paper will begin by introducing the scope of the study and providing key definitions. The second chapter details concepts that reappear in the literature on data and digital sovereignty alike. This paper's literature review presents essential ideas from the literature to contextualise the backdrop against which the case studies would make the most sense. The third chapter of this paper addresses differing methods of internet governance across jurisdictions. Thereafter, this paper brings our attention to India, trends in its digital policy, and its implications. The paper concludes with policy recommendations based on research of data sovereignty and internet governance.

Definitional Clarity:

Early discourse on the internet and cyberspace conceptualised it as a challenge to conventional understandings of boundaries and existing law. The internet existed outside the parameters of traditional sovereignty. As such, internet governance and legislation proved to be elusive and equally complex. However, recent years have seen changes as cyberspace becomes a space for political contestation. Public discourse has also shifted as the internet becomes filtered and fragmented; a concept termed 'balkanisation.'[1] Furthermore, the increasing involvement of technology in our daily lives has made this change almost inevitable. Thus, an examination and definition of these critical concepts are necessary to facilitate a nuanced discourse.[2]

Data sovereignty is a contested concept and largely this contestation is due to the varying communities discussed across – *political, industrial, and privacy*.[3] When defining data sovereignty, it is helpful to refer to the principles of sovereignty. Sovereignty comprises rights as well as obligations and these rights refer to both national and international rights. National rights are premised upon the notion that states may exercise power within their respective territories. Their actions within their jurisdiction are to their discretion and protected by their

1 Hill, Jonah Force. (2012). "A Balkanized Internet?: The Uncertain Future of Global Internet Standards." *Georgetown Journal of International Affairs*, 2012, 49-58. Available at: http://www.jstor.org/stable/43134338, (last accessed on June 14, 2021).

2 Lewis, James Andrew. "Sovereignty and the Evolution of Internet Ideology." *Center for Strategic and International Studies*. https://www.csis.org/analysis/sovereignty-and-evolution-internet-ideology, (last accessed on June 10, 2021).

3 Jarke, Matthias. (2020). "Data Sovereignty and the Internet of Production." *Advanced Information Systems Engineering*, 549–58. https://doi.org/10.1007/978-3-030-49435-3_34., 549, (last accessed on June 9, 2021).

sovereignty. Internationally, this sovereignty becomes more complex. The systems and institutions states participate within dictate the norms they follow.[4]

Data sovereignty has been conceptualised in different ways; it is "information which has been converted and stored in binary digital form ... subject to the laws of the country in which it is located", and it has also been defined as a "catch-all term to describe different state behaviours towards data generated in or passing through national internet infrastructure."[5] Data sovereignty is distinct from cyber sovereignty. Data sovereignty is a subclass of cyber sovereignty, defined as "the subjugation of the cyber domain to local jurisdictions." [6] While the cyber domain is a system with locational underpinnings, and each aspect of it is subject to the laws and jurisdiction of a given sovereign authority. Furthermore, while this brand of cyber sovereignty is recognisable within technical, social, judicial or geopolitical spheres, data sovereignty refers to states precisely constraining data flows to their respective national jurisdictions.[7] Cyber sovereignty would be a state's attempt at controlling and governing its cyber domain and infrastructure within state borders. This governance and control would include all features of cyber activity. Data sovereignty, separately, only considers the regulation of data flows within a nation-state. It is the management of data within a nation-state that is adherent to its respective laws, practices, and customs.[8]

Alternatively, Andrew Keane Woods, a legal scholar, characterises data sovereignty with a few elements extrapolated from the broader definition of sovereignty. [9] He notes that definitions of sovereignty feature aspects of "supreme control", "over a territory", and "independent from other sovereigns." [10] Ultimately, the key takeaway is that states have the capability for sovereign control over the internet.[11]

The literature on internet governance has been limiting in conceptualising what internet governance is, and as such, definitions are similarly narrow. For our purposes, we can broadly define *internet governance* as the dynamic rules, regulations, norms and expectations of the

---

4 Robin, Patrice. (2018). "Trend Analysis: Cyber Sovereignty and Data Sovereignty." *CSS Cyber Defense Project.* Available at: https://www.researchgate.net/profile/MarieBaezner/publication/325335882_Trend_Analysis_Cyber_Sovereignty_and_Data_Sovereignty/links/5bebbdc34585150b2bb4f0ef/Trend-Analysis-Cyber-Sovereignty-and-Data-Sovereignty.pdf, (last accessed on June 10, 2021).

5 Polatin-Reuben, Dana, and Joss Wright. (2014). "An Internet with BRICS Characteristics: Data Sovereignty And The Balkanisation Of The Internet", 1-10. Available at: https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben, (last accessed on June 14, 2021).

6 *Ibid*.

7 *Ibid*.

8 Snipp, C Matthew. (2016). "What Does Data Sovereignty Imply: What Does It Look Like?" In *Indigenous Data Sovereignty: Toward an Agenda*, edited by KUKUTAI TAHU and TAYLOR JOHN, 39-56. Acton ACT, Australia: ANU Press. Available at: http://www.jstor.org/stable/j.ctt1q1crgf.10, (last accessed on June 9, 2021).

9 Woods, Andrew. (2018). "Litigating Data Sovereignty". Yale Law Journal, 328 - 406.

10 *Ibid*.

11 *Ibid*.

internet. [12] The commonly referred to balkanisation of the internet is the process by which the internet is fragmented.[13]

Additionally, the concept of cyber exceptionalism may provide insight into the difficulties of governing the internet. Cyber exceptionalism implies that the digital sphere contains an inherently different quality or characteristic from the physical sphere. Cyber exceptionalism, while predominantly beginning in the 1990s, is still pervasive in discourse. In this paradigm, digital spaces cannot be regulated in the same manner as analogue.[14] Another critical concept to define is data localisation since it directly impacts cross-border flow of data and sheds light on a State's approach towards data sovereignty. Data localisation is the mandatory requirements of local data storage, which can either be stored exclusively locally or mirror data copies, which alter data flows.[15]

Models of Governance:

Reuben and Wright propose a binary of weak and strong data sovereignty approaches in their 2014 paper. [16] Weak data sovereignty is private sector-led, and strong data sovereignty prefers a state-led approach.[17] While this paper refers specifically to data sovereignty, this concept applies to the broader governance of the internet. Across global jurisdictions, countries have adopted varying levels of intervention from either state or private actors. Later in this paper, we will examine the approaches that China, Russia, the EU/UK, and the US have adopted to analyse how effective they have been through the lens of state versus private-led approaches to data protection and internet governance regimes.

In this context, multi-stakeholderism is a principle of state and non-state actors making policy decisions. Multi-stakeholder internet governance is characterised by decentralised procedures in decision-making which provided the space for varied actors to aid in the development of norms. In this model, governance would occur based on inclusion, collaboration and consensus-approved decision-making. [18]

---

12 Wilson, E. J. (2005). "What is Internet Governance and Where Does it Come From?" Journal of Public Policy 25: 29 – 50.

13 Hill, Jonah Force. (2012). "A Balkanized Internet?: The Uncertain Future of Global Internet Standards." *Georgetown Journal of International Affairs*, 2012, 49-58. Available at: http://www.jstor.org/stable/43134338, (last accessed on June 14, 2021).

14 Pohle, J. & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532 , (last accessed on June 9, 2021).

15 Kovacs, A., Ranganathan, N. (2019). Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India. Data Governance Network Working Paper 03.

16 Polatin-Reuben, Dana, and Joss Wright. 2014. "An Internet with BRICS Characteristics: Data Sovereignty And The Balkanisation Of The Internet", 1-10. Available at: https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben, (last accessed on June 14, 2021).

17 Polatin-Reuben, Dana, and Joss Wright. (2014). "An Internet with BRICS Characteristics: Data Sovereignty And The Balkanisation Of The Internet", 1-10. Available at: https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben, (last accessed on June 14, 2021).

18 Pohle, J. & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532 , (last accessed on June 9, 2021).

Multi-stakeholder arrangements in governance often refer to transnational and cross-border issues and predate the internet.[19] The multi-stakeholder model of internet governance emerged in 2005 during the UN World Summit on the Information Society (WSIS) when the Working Group on Internet Governance (WGIG) employed the term.[20] WGIG understood that then-current internet governance models were ineffective for participation from stakeholders. The multi-stakeholder model was a concession and compromise between private and public internet regulation. This multi-stakeholder concept rapidly proliferated in discourse and practices.[21] All countries' aspiration for multi-stakeholder governance is not shared, as demonstrated by the chosen case studies.

Another point of note is the impact of asymmetric technological and internet development in the West and its impact on multi-stakeholderism. This begets questions of how egalitarian this multi-stakeholder approach is and the implications for specific agencies and their locations. An example of this asymmetry is evident in ICANN which shall be elaborated upon later in this paper.

Indian Approach to Internet Governance and Existing Legislation:

To date, India has no omnibus legislation which addresses its issues of data privacy. The following doctrines are the ones in India that address the evolving conceptions of information privacy in India: *The Indian Copyright Act, 1957; **Information Technology Act, 2000**; Credit Information Companies Regulation Act, 2005; the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011;* and *the Personal Data Protection Bill, 2019*. Please note that this list does not include any court rulings. "The Personal Data Protection Bill, 2019" and "Report by the Committee of Experts on Non-Personal Data Governance Framework" are the two documents/legislation closest to addressing this. In this context, we find that the classification of data as personal and non-personal is also essential. Personal data is considered data where traits, characteristics, and other identifiers can be used for identification.[22] Non-personal data as defined by the "Report by the Committee of Experts on Non-Personal Data Governance Framework" is data which is not personal. The general definition provided is "data that never related to an identified or identifiable natural person" and "data which were initially personal data, but were later made anonymous. Data which are aggregated and to which certain data-transformation techniques are applied, to the extent that individual-specific events are no longer identifiable, can be qualified as anonymous."[23]

Issues with these delineations of non-personal and personal data become apparent through a critical review. Foremost, ambiguities on what classifies as non-personal data are of immediate

---

19 Hofmann, Jeanette. (2016). "Multi-stakeholderism in Internet governance: putting a fiction into practice." *Journal of Cyber Policy*, 1(1), 29-49, DOI: 10.1080/23738871.2016.1158303.

20 *Ibid.*

21 *Ibid.*

22 Michèle Finck and Frank Pallas. (2020). "They who must not be identified—distinguishing personal from non-personal data under the GDPR." *International Data Privacy Law*, Volume 10, Issue 1Pages 11–36, Available at: https://doi.org/10.1093/idpl/ipz026.

23 Report by the Committee of Experts on Non-Personal Data Governance Framework.

concern. Moreover, non-personal data is dubiously classified as not needing protection while personal data ought to be. Data is sensitive information that can be easily weaponised, regardless of its status as personal or non-personal.[24] For example, non-personal data could be misused against a community. We could take the example of a prevalent illness in an area, and this data then being used to increase insurance premiums. This scenario is a case of data being weaponised - data that is collected from people and used to their detriment. Misused information or sensitive personal information can be used to discriminate in cases that range from individuals seeking housing, to insurance, to immigration eligibility, to medical care, to loans.[25] We will later examine data use and misuse in more depth.

Before the proposal of "The Personal Data Protection Bill, 2019", personal data in India was governed by *Information Technology (IT) Rules, 2011,* which functions under the umbrella of the *Information Technology Act, 2000.* The *IT Act* now is outdated with the newer technologies and mechanisms for data usage and transfer and is not up to date with the existing technologies. Furthermore, the Non-Personal Data Governance Framework is the first of its kind as it creates a stark dichotomy between personal and non-personal data. It addresses non-personal data, but this delineation could prove problematic as will be discussed in the subsequent sections of this paper.

Conclusion:

This introduction introduced some essential topics that will be referenced later in this work. For the purpose of simplicity, the included are not exhaustive. However, these definitions are suitable for our purposes. The following chapter will be a Literature Review that will go over key concepts to understand digital and data sovereignty claims and internet governance.

2. Literature Review

Introduction:

If we understand best practices and approaches to internet governance and, as a by-product, protect data sovereignty, it is essential to review the existing literature. We will use the extant work to contextualise the scholarship on and history of fundamental aspects of internet governance. ICANN, its formation, evolving role, and contentions around it will be examined as an example of an attempt at global internet governance. We also consider and review data – types and usage. This section also includes an analysis of digital and data sovereignty. The courts' role in internet governance will also be explored.

---

[24] Singh, Shiv Shankar. "Privacy and Data Protection in India: A Critical Assessment." *Journal of the Indian Law Institute* 53, no. 4 (2011): 663-77. http://www.jstor.org/stable/45148583, (last accessed on June 8, 2021).

[25] Winter, Jenifer Sunrise. (2018). "Introduction to the Special Issue: Digital Inequalities and Discrimination in the Big Data Era." *Journal of Information Policy* 8: 1-4. doi:10.5325/jinfopoli.8.2018.0001.

Internet Corporation of Assigned Names and Numbers (ICANN):

For this analysis of the key actors and institutions in internet governance, we begin with an examination of ICANN which suffice to say ICANN is a crucial part of the global internet governance regime.

The Domain Name System (DNS) is an essential part of the worldwide internet infrastructure.

ICANN was formed in 1998 to govern the internet's infrastructure of domain name and Internet Protocol (IP) identifiers.[26] ICANN now plays a role that it transitioned into, which was once performed by IANA, or the Internet Assigned Numbers Authority.[27] ICANN's transition into its role was supported by the US Department of Commerce. As the organisation tasked with controlling the DNS, it is responsible for setting international widespread technology infrastructure guidelines,[28]and to put it in layman terms, ICANN's job is of practically organising the DNS of the internet.[29] In essence, the job of ICANN to control the DNS is a technical one.[30]

ICANN's connection to the US government and its power over the global web, and challenges to its legitimacy as an organisation, are very much part of the narrative of ICANN.[31] Foremost, its establishment and connection to the US government without being a US government organisation called into question its legitimacy as an institution made to perform procedural and policymaking DNS actions.[32] ICANN formed because of a government initiative. [33] This resulted from both the private sector and active internet community wanting to solve the disagreement over the governance of the DNS. At a point, the US government considered taking control of the DNS. However, this was reconsidered, and the government then allowed the private sector to take charge of the DNS.[34] ICANN set out to achieve its goal of governance with a highly representative constituency as its founders were optimistic about the global nature of the internet.[35] Through this understanding, it was apparent that the needs should inform the decision-making of its userbase. Thus, ICANN committed itself to the goal of having diverse and broad representation. ICANN also attempted to innovate through using the public in private-sector decision making.[36]

---

26 Weinberg, Jonathan. (2000). "ICANN and the Problem of Legitimacy." *Duke Law Journal* 50, no. 1: 187-260. (last accessed on June 2, 2021). doi:10.2307/1373114.

27 *Ibid*.

28 *Ibid*.

29 Palfrey, John. (2004.) The end of the experiment: How ICANN's foray into global internet democracy failed. Harvard Journal of Law & Technology 17(2): 409-473.

30 Weinberg, Jonathan. (2000). "ICANN and the Problem of Legitimacy." *Duke Law Journal* 50, no. 1: 187-260. (last accessed on June 2, 2021). doi:10.2307/1373114.

31 *Ibid*.

32 *Ibid*.

33 Palfrey, John. (2004.) The end of the experiment: How ICANN's foray into global internet democracy failed. Harvard Journal of Law & Technology 17(2): 409-473.

34 *Ibid*.

35 *Ibid*.

36 *Ibid*.

However, this goal of 'representation' and whether it was fulfilled is dubious. Moreover, the principle of 'openness' in ICANN is equally ambiguous. Openness has long been part and parcel of the writing on cyberlaw and remains a confusing notion. [37] In the space of the digital commons especially, openness and this associated idea of the internet which transcends borders, can be conflated and convoluted. Openness in this space has many implications, and ICANN has been asked to demonstrate as much.[38] Perhaps part of the issues of ICANN comes from its structure as an organisational body. ICANN was established as a body that mixed aspects of a corporation, standards body and government institution.[39]

ICANN's standing as a legitimate entity was questioned and continues to be under claims that ICANN singularly should not be able to have such control over DNS.[40]

Some scholars have questioned ICANN's venture into global governance as a non-government entity and its legitimacy, like John Palfrey[41] and Johnathan Weinberg.[42] ICANN endeavoured to validate its legitimacy through utilising the 'openness of the internet.[43] Its structure has permitted private entities to manage the DNS with input from users and input from states.[44] ICANN's role and accountability are more questionable still in countries that have strained relations with the US. We take the view that such an institution cannot exist in a vacuum separate from geopolitical tensions or issues that affect its country of incorporation.

Some argue that ICANN perpetuates a hegemonic structure in internet governance.[45] This is in direct opposition to the collaborative, multi-stakeholder model, which ICANN refers to and supports as a leading principle and ethos for internet governance.[46] Much has been written about ICANN, given its instrumental nature in the internet and internet governance canon. ICANN began in a purely technical capacity but has grown to occupy a politicised role. This is due to the evolution of ICANN and how international governments and communities have

---

37 *Ibid*.

38 "Openness Key Principle of Internet Governance Says UNESCO." (2004). http://www.unesco.org/new/en/member-states/single-view/news/openness_key_principle_of_internet_governance_says_unesco/, (last accessed on June 10, 2021).

39 Palfrey, John. (2004.) The end of the experiment: How ICANN's foray into global internet democracy failed. Harvard Journal of Law & Technology 17(2): 409-473.

40 Weinberg, Jonathan. (2000). "ICANN and the Problem of Legitimacy." *Duke Law Journal* 50, no. 1: 187-260. (last accessed on June 2, 2021). doi:10.2307/1373114.

41 John Palfrey, Clifford Chen, Sam Hwang, and Noah Eisenkraft. "Public Participation in ICANN." Available at: https://cyber.harvard.edu/icann/publicparticipation/, (last accessed on June 14, 2021).

42 Weinberg, Jonathan. (2011). *Governments, Privatization, and Privatization: ICANN and the GAC*, 18 Mich. Telecomm. & Tech. L. Rev. 189.

43 Palfrey, John. (2004.) The end of the experiment: How ICANN's foray into global internet democracy failed. Harvard Journal of Law & Technology 17(2): 409-473.

44 Palfrey, John. (2004.) The end of the experiment: How ICANN's foray into global internet democracy failed. Harvard Journal of Law & Technology 17(2): 409-473.

45 Van Klyton, Aaron and Soomaree, Ayush and Arrieta-Paredes, Mary-Paz, The Multistakeholder Model of Internet Governance, ICANN, and Business Stakeholders - Practices of Hegemonic Power (January 22, 2018). GigaNet: Global Internet Governance Academic Network, Annual Symposium 2017, Available at SSRN: https://ssrn.com/abstract=3107291, (last accessed on June 8, 2021).

46 ICANN. "About." *ICANN Public Meetings.* Available at: https://meetings.icann.org/en/about, (last accessed on June 5, 2021).

vied for alternative structures to internet governance.[47] While ICANN was established to promote international cooperation, it has caused tension internationally and sparked varying debates over its use.[48] Some countries take issue with ICANN's status as a non-profit incorporated in the United States and what this private entity represents as it has a large functional role in the operation of the internet.[49]

Data – Types, Use and Misuse:

Data is an unavoidable aspect of data sovereignty and internet governance. Conceptualisations of data are longstanding. In itself, data is a layer of information that affects everything. Data is also a concept often understood as disembodied and easily transferred from one medium to another. [50] This understanding of data, similar to understanding the internet as a borderless common, affects perception and regulation. It also conveniently negates the importance of power, political and social relations involved in this data. Furthermore, our perception of what is considered raw data is primarily a myth. We are constantly affected by our own biases and understandings, and our social order is a subjectively constructed idea.[51] For example, gender and race are man-made mechanisms for understanding our reality.

Data is often constructed and understood as a resource to exploit. This is apparent in both discourse and policy.[52] Importantly, data is not just collected and produced spontaneously. Instead, the market for data continues to grow, as do methods for data collection.[53] The lack of opportunities for dialogue and consent by individuals is challenging to navigate. Data sovereignty and internet governance are flawed concepts if the individual cannot be prioritised and protected. Community data is understood as a dimension of privacy dictated by a group. Community data, however, is loosely defined.[54]

The collection of data is an ever-present inevitability of participating in the cyber domain. Craig Mundie, former Senior Advisor to the CEO at Microsoft, presents that the rampant collection and storage of personal data is a constant and a given. People provide data to many organisations daily, whether they are government agencies, ISPs, or telecoms companies or financial firms. Data is often collected through passive means or when data is provided for one use while performing another action. Mundie terms this creation of data as a by-product as

---

47 Kesan, Jay P. and Gallo, Andres. (2008). "Pondering the Politics of Private Procedures: The Case of ICANN" (November 6, 2007). *I/S A Journal of Law and Policy*, Vol. 4, pp. 345-409, Illinois Public Law Research Paper No. 07-11, Available at SSRN: https://ssrn.com/abstract=1028128, (last accessed on June 10, 2021).

48 Baird, Zoë. (2002.) "Governing the Internet: Engaging Government, Business, and Nonprofits." *Foreign Affairs* 81, no. 6: 15-20. doi:10.2307/20033341.

49 Chatham House. (2016). *Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance: Research Volume Two Global Commission on Internet Governance.* Available at: https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202%20WEB.pdf. , (last accessed on June 12, 2021).

50 Kovacs, A., Ranganathan, N. (2019). Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India. Data Governance Network Working Paper 03.

51 *Ibid.*

52 *Ibid.*

53 *Ibid.*

54 *Ibid.*

"data exhaust." [55] Indeed, data collection is inevitable, as is our 'data exhaust.' In light of this, conversations around data should focus on the minimisation of data misuse and abuse rather than positing extreme positions such as banning cross-border flow or mandating data sharing.

What constitutes data misuse? Data misuse is data used inappropriately as compared to when the data was first collected.[56]

Enumerated below are a few examples to illustrate misuse of data:

- **Social Media and Content Recommendation:** Machine Learning and AI based content recommendation systems created by social networks such as Facebook and news aggregators like Google News were used to spread fake news to influence the US Presidential Elections in 2016.[57] In this widely reported incident, data collected through browsing and social media was used to target individuals based on their behaviour and psychographic profile. This effectively meant persuading voters through political messages catering to an individual's basal fears and beliefs to generate a favourable outcome.

- **Location Tracking:** The 2014 Uber case of an executive using a mechanism on the Uber application to track the whereabouts of a journalist and, more concerningly, the general use of the 'God Mode' setting. This setting enabled users to see all the Ubers in a city and the silhouettes of waiting Uber users who have flagged cars. If the users remained anonymous, it may have been a harmless addition to the application. However, an attendee later stated that Uber also allowed guests whereabouts and movements of 30 Uber users in New York in real time.[58] This is a classic case of user data being 'misused' to enable cybercrime such as 'stalking'.

- **Sale of Privileged Information without Consent:** AT&T call-centre workers sold privileged information (customer names and Social Security numbers) to third parties to unlock the phones.[59] This occurred in overseas call-centres where hundreds of thousands of customers records were sold. These data breaches spanned months and the sales of these

---

55 Mundie, Craig. (2014). "Privacy Pragmatism: Focus on Data Use, Not Data Collection." *Foreign Affairs* 93, no. 2: 28-38. Available at: http://www.jstor.org/stable/24483581, (last accessed on June 5, 2021).

56 "5 Examples of Data & Information Misuse." *ObserveIt.* Available at: https://www.observeit.com/blog/importance-data-misuse-prevention-and-detection/, (last accessed on June 7, 2021).

57 "Cambridge Analytica's Facebook Data Abuse Shouldn't Get Credit for Trump." (2018). *The Verge.* Available at: https://www.theverge.com/2018/3/20/17138854/cambridge-analytica-facebook-data-trump-campaign-psychographic-microtargeting, (last accessed on June 7, 2021).

58 Hill, Kashmir. (2014). "'God View': Uber Allegedly Stalked Users for Party-Goers' Viewing Pleasure (Updated)." *Forbes.* Available at: https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/?sh=bc90ad931411, (last accessed on June 8, 2021).

59 Fung, Brian. (2015). "AT&T will pay $25 million after call-center workers sold customer data." *Washington Post.* Available at: https://www.washingtonpost.com/news/the-switch/wp/2015/04/08/att-will-pay-25-million-after-call-center-workers-sold-customer-data/, (last accessed on June 14, 2021).

customers records and information lasted from November 2013 into April 2014.[60] This is an egregious breach of privacy.

- **Abuse of Data Access:** Officer Amy Krekelberg brought suit against the Minneapolis Police Department. According to the suit, officers had misused access to their police database to access personal data about Krekelberg. Krekelberg alleged that 58 officers had violated federal privacy by searching for her information and had also caused her emotional duress. Krekelberg was awarded $585,000.[61] This case demonstrates that unfettered access for law enforcement officials may have disastrous consequences and impressed upon the need for regulations around data access even in the case of law enforcement officials.

When data is misused, large sets of personal and non-personal data have consequences for those whose data it has collected. Large data sets contain patterns and correlations that allow algorithms to function and make predictions. Thus, even if data is missing, points can be inferred through other functions by these algorithms. These patterns and correlations can also provide information outside a given dataset – as data can be matched through proxy variables where correlations are strong enough. In sum, data about people is full of patterns. Patterns make a prediction and the imputation of missing data possible.[62]

Social identifiers have a known impact on many life outcomes, ranging from educational attainment to life expectancy. Algorithms make decisions through patterns. When parts of people's lives are recorded as information and patched together, common characteristics are grouped. These patterns can be related to a single person's data as autocorrelations when an individual has information collected repeatedly over time or patterns persist in communities or across people. These correlations exist amongst those who interact or communicate with each other.[63] Databases that collect data about people contain many patterns and correlations. Many computer programs process information and learn through patterns; these programs include artificial intelligence and machine learning programs. The function of these programs can vary, whether they are to categorise, rank or make decisions about varying people or groups.[64] Social identifiers, like race, gender, caste, are pervasive, and machine learning algorithms can learn their correlates quickly when trained on past data and thus, excluding social categories and data is futile. Or, attempting to protect community data through excluding certain categories is not guaranteed to work.[65]

---

60 Gross, Grant. (2015). "AT&T call centers sold mobile customer information to criminals." *Computer World.* Available at: https://www.computerworld.com/article/2907223/att-call-centers-sold-mobile-customer-information-to-criminals.html, (last accessed on June 11, 2021).

61 "US: Police Found to Violate Fellow Officer's Privacy: Minnesota Case Shows Need for Stronger Data Protection Laws." (2019). *Human Rights Watch.* Available at: https://www.hrw.org/news/2019/06/20/us-police-found-violate-fellow-officers-privacy, (last accessed on June 10, 2021).

62 Williams, Betsy Anne, Catherine F. Brooks, and Yotam Shmargad. (2018). "How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications." *Journal of Information Policy* 8 78-115, (last accessed on June 14, 2021). doi:10.5325/jinfopoli.8.2018.0078.

63 *Ibid.*

64 *Ibid.*

65 *Ibid.*

Social identifiers and sensitive information remain rooted within big datasets regardless of attempts to delete or 'forget' them. If an algorithm is fed certain social category information, but it is not specifically designed to avoid discrimination, resultant outcomes are biased.[66] For instance, it was observed that while Amazon was using an AI enabled recruiting software the software was biased towards male candidates since its model was trained on a dataset containing information from mostly male candidates.[67] Consequently, the software downgraded resumes from female candidates. Another notable example is the use of machine learning based criminal risk scores used in different US jurisdictions to ascertain the likelihood of recidivism by an offender. The risk scores generated by the algorithms appeared to be biased against black offenders.[68]

Thus, removing categories is not a fruitful outcome nor does it prevent harm.[69] Algorithmic decision-making relies on correlations. These relationships can link a person's characteristics, past actions, social contacts, and categories to others. These processes can replicate discrimination or assumptions based on membership in a group, and this can happen regardless of whether certain data is intentionally withheld or removed.[70]

Data often cannot be made wholly anonymous, as algorithms and machines can re-identify anonymised data. Given the sensitivity of data and its collection, the continued centralisation of collected information and intelligence seems to be most dangerous, especially when considering lacking accountability mechanisms for this data. The critical endeavour is establishing a surveillance-privacy balance that conforms to India's political norms and the rights awarded to citizens within the Indian democracy.[71]

Strategies of data protection and governance often propose theories based on privacy as a justification. However, one could argue discrimination or its potential serves as a better justification for revaluating surveillance and other data collection mechanisms.[72] Historically, focusing on privacy is unlikely for reframing policy and making alternate suggestions because it lacks the gravitas to conquer arguments that often cite national security or profitability of businesses as reasons to allow data collection, storage and surveillance. Instead, freedom from

---

66 *Ibid*.

67 Dastin, Jeffrey. (2018). "Insight – Amazon scraps secret AI recruiting tool that showed bias against women." *Reuters.* Available at: https://in.reuters.com/article/amazon-com-jobs-automation/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idINKCN1MK0AH, (last accessed on June 14, 2021).

68 Angwin, Julia, Larson, Jeff, Mattu, Surya, and Kirchner, Laura. (2016). "Machine Bias." *ProPublica.* Available at*:* https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, (last accessed on June 13, 2021).

69 Williams, Betsy Anne, Catherine F. Brooks, and Yotam Shmargad. (2018). "How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications." *Journal of Information Policy* 8 78-115, (last accessed on June 14, 2021). doi:10.5325/jinfopoli.8.2018.0078.

70 *Ibid*.

71 Ünver, Akin. (2018). "Politics of Digital Surveillance, National Security and Privacy." Available at: https://edam.org.tr/wp-content/uploads/2018/04/Chrest_Surveillance2.pdf, (last accessed on June 14, 2021).

72 Cramer, Benjamin W. (2018). "A Proposal to Adopt Data Discrimination Rather than Privacy as the Justification for Rolling Back Data Surveillance." *Journal of Information Policy* 8: 5-33. Accessed June 14, 2021. doi:10.5325/jinfopoli.8.2018.0005.

discrimination could be used as a better value and position to argue in favour of better oversight mechanisms.[73]

The Scope of Sovereign Authority Over the Cloud:

The internet has long appeared to be defiant to norms of conventional sovereignty models. Traditionally understood structures of territoriality become, in some ways ineffective, with the innovations of the internet. At least, this became a popularised idea in the 1990s.[74] However, ideas of sovereignty over the internet have changed as technology has developed. States have established national laws and other forms of intervention to exercise their sovereign authority.[75]

States can heavily regulate the internet and exercise their sovereignty and control in their territory.[76] More detailed examples of this will be apparent later in this paper. In some cases, this control can be exerted through physical mechanisms.[77] The prior understandings of the internet as a boundless and borderless commons no longer holds. States have tools that can inform internet governance. For example, states can control the internet through the physical construction of the network. This network architecture includes fiber, severs, and computers, constituting the internet within a state's borders. These tools allow a state to censor content, monitor and restrict a state's access to the network. [78] Notably, this form of control is a cruder method and can be bypassed.

There are several conceptualisations of internet governance, which can be simplified into two groups. One ideal also known as the cosmopolitan ideal aspires for one set of rules and laws to govern the internet versus the sovereign-difference ideal, which aspires for an internet that operates differently in different places. The first ideal, or the cosmopolitan, is premised on the notions of free, liberalised internet.[79] In reality, the actual structure of the internet looks more like the sovereign-difference ideal. Internet governance structures vary across different states. However, these differences can become points of conflict with the other states.[80]

The sovereign-difference ideal focuses primarily on a state's ability to exercise power over its internet locally. This sovereign-difference ideal is present in China and Russia. The cosmopolitan ideal is most apparent in the internet governance of the US. There is also scholarship that notes that this ideal of rules that govern all the internet can is a form of Western and American imperialism.[81] Whereas the counterargument often includes the danger of the 'splinternet' or the balkanisation of the internet. However, sovereign-difference and

---

73 Cramer, Benjamin W. (2018). "A Proposal to Adopt Data Discrimination Rather than Privacy as the Justification for Rolling Back Data Surveillance." *Journal of Information Policy* 8: 5-33. Accessed June 14, 2021. doi:10.5325/jinfopoli.8.2018.0005.

74 Pohle, J. & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532 , (last accessed on June 9, 2021).

75 *Ibid.*

76 Woods, Andrew. (2018). "Litigating Data Sovereignty". Yale Law Journal, 328 - 406.

77 *Ibid.*

78 *Ibid.*

79 *Ibid.*

80 *Ibid.*

81 *Ibid.*

cosmopolitanism are not mutually exclusive in the internet governance question. Proof of this is that both these models exist and have previously been implemented by states.[82]

Digital Sovereignty – A Concept:

Digital sovereignty has varying connotations.[83] Its changing characteristics correspond to the different states and actors involved in these conceptualisations. Thus, claims for digital sovereignty also differ. Digital sovereignty claims can be understood across to what extent they "address the capacity for digital self-determination by states, companies or individuals." [84]

One type of digital sovereignty claims focuses on the idea that a nation or area should be able to take self-governing action and accordingly make policy decisions on its digital infrastructure.[85] Many claims for digital sovereignty centre on locational restricting of sovereignty to specific territories so states can continue to ensure digital infrastructures and authority regarding digital communication matters relating to their territories and citizens.[86]

Democratic notions of digital sovereignty vary greatly from governments with a more traditionally authoritarian approach.[87] We take the example of China, which assumes the proliferation of global communication and openness as a threat to its political status quo.[88] China responded to the increase of global communication by promoting and developing its brand of digital sovereignty.[89] This type was framed as *cyber sovereignty* or *internet sovereignty*. [90] The types of claims made by China was similarly adopted by Russia, as this paper will later demonstrate.[91] ‘'Western' states addressed the need for control and independence in the cybersphere in different ways. The justification for these claims was based mainly on security matters. As global interconnectedness grew, states became aware of new types of vulnerabilities.[92] For example, malicious software or 'malware' - the first piece of malware, the Creeper worm, was created in 1971.[93] Growing concern over cybersecurity has grown in cyber discourse, and this unease has been voiced by scholars, politicians and security officials alike.[94] These newer vulnerabilities have led to the growing claims and assertations for digital/cyber sovereignty.

---

82 *Ibid.*
83 Pohle, J. & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532 , (last accessed on June 9, 2021).
84 *Ibid.*
85 *Ibid.*
86 *Ibid.*
87 *Ibid.*
88 *Ibid.*
89 *Ibid.*
90 *Ibid.*
91 *Ibid.*
92 *Ibid.*
93 Martindale, Jon. (2018). “From pranks to nuclear sabotage, this is the history of malware.” *Digital Trends.* Available at: https://www.digitaltrends.com/computing/history-of-malware, (last accessed on June 14, 2021).
94 Wulf, W. A., & Jones, A. K. (2009). Reflections on Cybersecurity. *Science,* 326, no. 5955, 943-944.

These claims through government-practices are increasingly trending toward proposals for data localisation. These practices focus on limiting the storage, exchange, and/or processing of data to jurisdictions. The premise of these claims is often based on the need to ensure foreign intelligence agencies and commercial agencies may have to certain types of data only. [95] Attempts at data localisation practices have received criticism on the basis that these moves would ruin the 'openness' of the internet and contribute to the growing 'splintering' or 'Splinternet' as it has been termed.[96]

Pushes for digital sovereignty have also been claimed with emphasis on economic autonomy. These claims for digital sovereignty focus on the self-sufficiency of a state's national economy without the need for foreign technology and service providers. These claims are often a response to the seemingly apparent power dynamics of the current market where the US and China have market dominance.[97] The instruments that governments utilise to account for these differences can share similarities with the claims for digital sovereignty that focus on fortifying the security of technological systems and national autonomy. However, when claims focus on economic autonomy, these attempts at digital sovereignty focus on transforming fundamental aspects of the economy.[98] Specific measures then focus on digital trade and specifically attempt to control commerce and data flow delivered through networks.[99]

Other claims for digital sovereignty can focus on discourses surrounding user rights and laws and protect the consumer, focusing on the norms of a country. Some countries' plan for digital sovereignty can contribute to more extensive conversations which critically interrogate the power dynamics of history and its contribution to today, like the use of terms like digital imperialism or digital colonialism.[100]

Newer claims of digital sovereignty focus on empowerment of the user, user autonomy and individual self-determination.[101] The idea that the internet and the web were incompatible with state sovereignty has remained, especially in the public conscious. Despite this, state actors have emphasised the necessity to establish sovereignty digitally.[102]

Part of this shift is related to the changing power dynamics of cyberspace. This is most easily seen in the immense amount of power specific corporate entities now hold.[103] Moreover, the goals of these entities are different from the decentralised institutions that were meant to govern the internet. Instead, these entities capitalise on the possession of digital goods like data and even societal infrastructures.[104] A few specific digital platforms and intermediaries control the lion's share of the available content on the internet, rendering the 'openness of the internet

---

95 Pohle, J. & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532 , (last accessed on June 9, 2021).
96 *Ibid.*
97 *Ibid.*
98 *Ibid.*
99 *Ibid.*
100 *Ibid.*
101 *Ibid.*
102 *Ibid.*
103 *Ibid.*
104 *Ibid.*

largely conceptual.[105] The monopoly that these 'few' have make them incredibly difficult to regulate and exercise sovereignty over. From a legislative standpoint, the global span of these few makes it difficult. Furthermore, these corporations provide desirable foundations for greater society from a practical standpoint, causing interference at critical junctures with nation-states own governance. For example, communication mechanisms done via internet corporations cannot be structured and regulated in the same manner as their less modern counterparts.[106] These new constructions have energised discourse about the changing landscape of world orders and have led to questioning how governance could work with this.[107]

We can also understand digital sovereignty in two buckets. These sovereign powers are the "powers to compel compliance" and the "powers to control the means of compliance."[108] Wherein compelled compliance allows businesses and users to design and use the internet as they wish under the condition they comply if the government wishes to act. Controlled compliance pre-empts actions, and the state informs internet companies on how to act in the first instance. The key difference here is that in compelled compliance instances, law enforcement/the government allows the businesses the opportunity to comply before taking action. In the other exercise of power, businesses have to allow access to a platform by weakening their security protocols. In controlled compliance, the state determines all operation with limited choice for businesses.[109] States will opt for controlled compliance, typically when compelled compliance is ineffective.[110]

Sovereign State Interests in Internet Governance:

Much of the literature highlights how the internet is challenging sovereign deference structures. Regulating the internet and the internet economy has become an increasingly contentious issue. Conflicts between governments and third parties often arise when compelled compliance fails. This has occurred with WhatsApp in a few instances and other big tech platforms in foreign countries, where local laws or local law enforcement has attempted to compel compliance but has failed. For example, in 2017 France directed WhatsApp to stop sharing user data with Facebook with threat of sanctions.[111] State governments wish to enforce their laws within their jurisdiction with opposition from the given American firms. [112]

---

105 *Ibid.*
106 *Ibid.*
107 *Ibid.*
108 Woods, Andrew. (2018). "Litigating Data Sovereignty". Yale Law Journal, 328 - 406.
109 *Ibid.*
110 *Ibid.*
111 Gibbs, Samuel. (2017). "France orders WhatsApp to stop sharing user data without consent." *The Guardian.* Available at: https://www.theguardian.com/technology/2017/dec/19/france-orders-whatsapp-stop-sharing-user-data-facebook-without-consent, (last accessed on June 1, 2021).
112 Woods, Andrew. (2018). "Litigating Data Sovereignty". Yale Law Journal, 328 - 406.

The Judiciary:

In the literature, there is an ongoing debate on whether global internet governance issues should be and can be appropriately addressed by the courts[113] The system that courts work within is not, by design, meant to settle these notable technological policy issues.

Courts have historically handled cases concerning sovereignty and deference to sovereign nations. The issues that arise with data sovereignty, in many respects, are not that different. The methods used to mitigate issues of sovereignty are similar to those available to resolve data sovereignty issues.[114] The ongoing debate on whether sovereignty limits extraterritorial exercises of power remain open-ended in applying the principle of sovereign deference.[115]

Andrew Keane Woods has written on this matter extensively. In one work, he argued that courts should utilise the conflicts-of-laws principle or simply, balancing competing governments' interests against one another.[116] Government interest refers to an interest in the context of sovereignty when understanding this beyond law enforcement and in cross-border disputes regarding the internet.[117]

Issues that often arise in cross-border disputes include injunctions and takedowns for extremist content,[118] delisting and the right to be forgotten,[119] requests by law enforcement for foreign-held data, [120] surveillance, [121] and digital trade limitations.[122] Some of the problems in addressing these issues arise from the digitisation of previously understood areas of law.[123] Another critical area is how to deal with the 'cloud' and issues of jurisdiction on the cloud.[124] The new form of the principle of conflicts of laws, when dealing with extraterritorial issues, complicates issues regarding where content is produced and then consumed and which country or state would be protected.[125]

The ongoing conflicts of sovereignty which arise in internet governance could mean courts need to use sovereign-deference doctrines in these issues. Andrew Keane suggests the utility of comity doctrines which are foreign relations doctrines.[126] *Comity* is a concept which appears in American foreign relations law. It is a principle that honours courts should acknowledge and defer to the sovereign interests of other states.[127] Comity is a form of diplomacy which is assumed. It can be simply understood as the choice to defer to the interests of a foreign

113 *Ibid.*
114 *Ibid.*
115 *Ibid.*
116 *Ibid.*
117 *Ibid.*
118 *Ibid.*
119 *Ibid.*
120 *Ibid.*
121 *Ibid.*
122 *Ibid.*
123 *Ibid.*
124 *Ibid.*
125 *Ibid.*
126 *Ibid.*
127 *Ibid.*

government actor even when it is not required by international law.[128] Comity can foster better relations and encourage cooperation.[129] Comity doctrines have developed over time as a result of interactions between countries' legal systems. [130]

3. Differing Methods of Internet Governance Across Countries

Introduction:

The purpose of this chapter is to illustrate how different countries have approached internet governance and their respective data protection and sovereignty regimes. We will examine the case studies of China, Russia, the EU/UK, and the USA. The Indian approach would be examined in the subsequent chapter. This section aims to demonstrate the different methods of internet governance in regions, their respective difficulties, and how these regions have accommodated political and cultural norms. Given the difference in each region's approach, the analysis of these respective regions has been tailored to what has been highlighted as pertinent.

The methodological approach to selecting these countries was based on a few characteristics of each respective country. China was selected as it has demonstrably one of the largest populations of internet users. Furthermore, its internet governance model is an example of 'strong' governance enforced by the state.[131] The case study of Russia was selected for similar reasons; Russia's internet governance, again, is strongly impacted by state mechanisms of control. The EU/UK example was selected based on the robust General Data Protection Regulation (GDPR) to examine the efficacy of this piece of legislation. The US was selected since it is home to the big technology giants, impacting all discussions on data regulation and moderation while lacking omnibus legislation. The overarching goal of this chapter is to compare distinct approaches adopted by various states with respect to data sovereignty and we have selected countries that vary from ostensibly ‘strong’ state control to largely ‘citizen’ focused models since we believe that this would facilitate analysis of different types of data sovereignty regimes.

3.1 China

China is a behemoth member of global cyberspace with the largest population of internet users - 850 million.[132] China's relationship with internet usage is often understood as a repressive and restrictive regime. However, the reality of China's internet is more complex than what is initially understood. Discourse on China's approach to internet control often frames China's approach as the diametric opposite of the US’ model. These discussions focus on concepts of

---

128 *Ibid.*

129 *Ibid.*

130 *Ibid.*

131 Polatin-Reuben, Dana, and Joss Wright. (2014). "An Internet with BRICS Characteristics: Data Sovereignty And The Balkanisation Of The Internet", 1-10. Available at: https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben, (last accessed on June 14, 2021).

132 https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/, (last accessed on June 5, 2021).

Chinese "internet sovereignty" at odds with American "internet freedom." Though this framing can illustrate aspects of China's internet policy, it is reductive and cannot encompass the more intricate elements of China's internet governance regime.[133]

The growth and penetration of the internet in China has promoted a growing number of government agencies and policies. Internet governance at the domestic level includes regulations designed to protect the security of the country or industry. Less attention is given to individual rights, such as privacy protection. These objectives reflect the intention of reinforcing government control and regulatory power over the internet. Some particular elements stand out, for instance China uses ISPs that are guided through "choke points" or network nodes for centralised control.[134] This centralised control mechanism allows the Chinese government to regulate and protect its cyber sovereignty tightly. Chinese internet governance also relies on buy-in from citizens who participate in their governance.[135] Chinese citizens must adhere to these norms and laws for this internet governance to be effective.

In-depth historical analyses of China's policy reveal an evolving and adapting method for internet governance. A landmark event in 2010 drastically changed the landscape and relationship China had with the internet and international players.[136] In 2010, Google publicised it would no longer censor results in Mainland China and may even remove itself altogether.[137] At this point, the then US Secretary of State, Hilary Clinton, suggested that the Chinese government was building its own "new virtual Berlin wall" oppositional to the tenets of 'American' internet freedom.[138] China also stated that the USA should halt imposing its "information imperialism."[139] This notion of information imperialism is not novel and, Post-colonialist critical discourse has engaged with the concept of new forms of imperialism and colonisation by the 'West' of the global South. This information imperialism and digital colonisation are asserted through information flows and digital technology production of the West. [140] In the aftermath of these events, China issued its first White Paper on internet governance. This White Paper elucidated a clear position on the global internet and demarcated a departure from its previous paradigm.[141]

The White Paper details the Chinese government's commitment to internet development and accessibility. It also suggests that the internet will support both the economic and social

---

133 Hong Shen. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication* 9:3, pages 304-324.

134 Epifanova, Alena. (2020). "Deciphering Russia's "Sovereign Internet Law."" DGAP Analysis 2, 11 p. Available at https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf, (last accessed on June 14, 2021).

135 Hong Shen. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication* 9:3, pages 304-324.

136 *Ibid.*

137 *Ibid.*

138 *Ibid.*

139 *Ibid.*

140 Kwet, Michael. (2019). "Digital Colonialism: US Empire and The New Imperialism in The Global South". *Race & Class* 60 (4): 3-26. doi:10.1177/0306396818823172.

141 Hong Shen. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication* 9:3, pages 304-324.

development of China. It notes how both IT and the internet have made massive contributions to the rapid growth of the Chinese economy. In the White Paper's third section, the paper notes that the Chinese government is committed to safeguarding the convenience for people to exercise their rights on the internet. The section, Basic Principles and Practices of Internet Administration, states that the main objectives of China's internet administration are to promote convenient internet accessibility, healthy growth, online freedom of speech, and govern the order of information spread. It states that China regulates its internet by law and protects its citizens' digital privacy. The Chinese government will continue to amend its internet administration, it says, led by rational and scientific law-making. The White Paper highlights that the internet of different countries belongs to distinct jurisdictions regarding its international interactions. It upholds the idea that all countries should dynamically interact and cooperate to support internet developments. Through the White Paper, it is reinforced that China will adhere to its "opening-up" policy and open its Chinese internet market with respect to its law and welcome other countries should they abide by its laws.[142]

Even though popular discourse has framed Chinese internet policy as narrow and an 'intranet', its stated objectives and ambitions are driven by many ambitions with the hope for outcomes beyond creating an isolated cybersphere. Its position is not purely a "heavy-handed authoritarian state motivated by the drive to elevate governments and intergovernmental organisations as the sole governors of the global internet."[143] Rather; its governance can be better understood as the result of multi-layered engagements between a group of stakeholders, which range from state agencies and business units in domestic and international settings. The vested interests of multiple state agencies have impacted governance. Furthermore, the ongoing Chinese attempts to centralise its internet policy is the outcome of this domestic competition. One can also not disregard the impact of substantial Chinese companies like Huawei and Alibaba and the impact of their agendas in China's internet governance discourse. The power of behemoth companies like Huawei and Alibaba readily affect and shape the internet governance agenda. These complex power relations between state and business are a more apt reflection of the factors at play when reviewing the Chinese approach to internet governance.[144] The Chinese government is aware of its reliance on these big players to maintain its 'sovereign' technological structure.

Its own internal struggles with power-players have informed the Chinese approach to internet governance. The significance corporations like Huawei cannot be discounted when reviewing how the global market of internet infrastructure is being impacted.[145] Huawei is one of the

142 http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207975.htm/, (last accessed on June 5, 2021).

143 *Ibid*.

144 Hong Shen. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication* 9:3, pages 304-324.

145 Séverine Arsène. The impact of China on global Internet governance in an era of privatized control. Chinese Internet Research Conference, May 2012, Los Angeles, United States.

largest sellers of 5G technology and smartphones in the world.[146] There are worries that Beijing could abuse Huawei's position as a Chinese company for espionage.[147]

The idea that China preferences national sovereignty over the internet and the existence of a censorship system called the "Great Firewall of China" may well be misleading.[148] In fact, in a 2010 White Paper, the Chinese government make statements about the internet as a tool for growth and developing national strength.[149]

Chinese internet governance is controlled primarily by the internet actors themselves. Chinese regulation of the internet is based on intermediary liability. Essentially, ISPs are liable for the publications of their users. This form of censorship is not entirely perfect, and many counter-censorship strategies exist. Furthermore, the speed at which information spreads makes this system even more lacking. It should be observed that the vital part of internet governance within China is dependent on the subscription to the social contract fostered by the Chinese Communist Party (CCP). The manner of control and observance of social norms re-enacted daily is a form of governance where individuals enable their control.[150]

Ultimately, while the goal is not to build an isolated Chinese internet – the Chinese government is responsible for the control and infrastructures of the internet within China. The government also opposes disruptions of their control of the internet. Internet control is firmly related to internet sovereignty. [151] China's method of internet governance is at odds with the multi-stakeholder model, which appears globally in the internet sector.[152]

The multi-stakeholder model is contradictory to China's model of internet sovereignty. The Chinese government asserts that internet governance should remain inter-governmental.[153] The Chinese government wishes for a governance model that guarantees its sovereignty over internet activities in China and with the Chinese government remaining as the only legitimate representative of Chinese internet users' interests. However, the characterisation that China wishes to build an intranet is incorrect. [154]

The Chinese approach to global internet governance is nuanced, as demonstrated by its long-term interactions and participation with ITU and ICANN. Within the ITU, the Chinese government is represented by its Ministry of Industry and Information Technology, the private sector by 37 companies, and the academic sector by nine universities and other institutes.[155] Within ICANN, the Chinese are mainly represented by registrars, with four politicians

146 https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant/, (last accessed on June 3, 2021).
147 *Ibid.*
148 Séverine Arsène. The impact of China on global Internet governance in an era of privatized control. Chinese Internet Research Conference, May 2012, Los Angeles, United States.
149 *Ibid.*
150 *Ibid.*
151 *Ibid.*
152 *Ibid.*
153 *Ibid.*
154 *Ibid.*
155 Negro, Gianluigi. (2020). "A history of Chinese global Internet governance and its relations with ITU and ICANN." *Chinese Journal of Communication*, 13:1, 104-121, DOI: 10.1080/17544750.2019.1650789.

representing the Chinese political sphere.[156] Data from varying stakeholders shows Chinese scholars and NGO managers demonstrating distrust of the US influence over ICANN. However, these people still supported a multi-stakeholder approach.[157]

China's strategy for development was released in March of 2021 – which included its ambitions for the technology. Huawei is heavily involved in these plans, including 6G reinforcing the giant's inextricable link to the government.[158]

3.2 Russia

Russian internet governance is focused on increasing control and isolation. Beginning in the late 1990s, Russia has increasingly promoted the supremacy of its own national and intergovernmental organisations to govern the internet.[159] The legislations of the last few years suggest a continued attempt to isolate the Russian internet and create more of an 'intranet'.

In recent years, Russia has expanded laws and regulations on internet infrastructure, digital content, and privacy of communications.[160] The following section will examine this legislation and its implications for the larger cyber community and dissecting trends in internet governance.

The Russian approach to the internet is focused on two pillars, namely control and increasing isolation. Authorities in Russia are continuing to expand their ability to filter and block internet content routinely. Internet laws have required ISPs in Russia to install equipment that provides authorities with the ability to evade providers and directly block content while rerouting digital traffic.[161] The federal communications authority installed necessary equipment across Telecommunications Service Providers (TSPs) and ISPs to facilitate such oversight.[162]

Since 2017, there have been trends in laws and regulations which increase the Russian government's control over their 'sovereign' internet. These laws build on each other and suggest a continued trend for the government to exercise stricter control over internet infrastructure and activity in Russia. These laws range from prohibiting VPNs and internet anonymisers to laws on the identification of messaging application. In May of 2019, Putin signed amendments

156 *Ibid.*
157 *Ibid.*
158 Available at: http://www.chinadaily.com.cn/a/202103/20/WS60554052a31024ad0bab0636.html/, (last accessed on June 8, 2021).
159 Budnitsky, Stanislav. (2020). "Toward a Cultural Framework of Internet Governance: Russia's Great Power Identity and the Quest for a Multipolar Digital Order." *CARGC Papers*. 13. https://repository.upenn.edu/cargc_papers/13.
160 "Russia: Growing Internet Isolation, Control, Censorship." (2020). *HRW.* Available at: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship#:~:text=Russian%20internet%20users.-,The%20Sovereign%20Internet%20Law,state's%20control%20over%20internet%20infrastructure, (last accessed on June 7, 2021).
161 *Ibid.*
162 Doffman, Zak. (2019). "Putin Now Has Russia's Internet Kill Switch to Stop U.S. Cyberattacks." Available at: https://www.forbes.com/sites/zakdoffman/2019/10/28/putin-now-has-russias-internet-kill-switch-to-stop-us-cyberattacks/?sh=6562fc2c31b2, (last accessed on June 10, 2021).

to two federal laws, titled *On Communication*[163] and *On Information, Information Technologies, and Information Security*[164], establishing critical digital infrastructure within Russia. This would later be called the Sovereign Internet Law.[165] Essentially through these laws, the government seeks to censor content it 'deems illegal'. And, in March of 2021, the Magistrate's Court of Moscow filed individual cases against Facebook, Google, Twitter, TikTok and Telegram that could lead to administrative fines worth an estimated US$54,000. This was in response to the platforms failing to delete allegedly 'illegal' content that incited teenagers to join protests and for spreading misinformation about police brutality.[166]

As such, there is no single law that denotes Russia's "Sovereign Internet Law" – instead, there are a series of amendments to existing laws that constitute the whole. Some of these amendments that seek to secure the Russian internet include:

i. installing technical equipment to respond to threats,

ii. centralising the management of telecommunication in case of a threat, and

iii. monitoring connection lines crossing the border of Russia and implementing the Russian national DNS.[167]

Currently, Russia's information and internet policy has notably tried to control the internet through restrictive internet laws. However, impediments have occurred due to practical considerations.[168]

These newest series of amendments require the establishment of a national DNS. The law would require ISPs from January 1st onward to use the national DNS. Requiring ISPs to use the DNS would allow Russian authorities to manipulate results provided to the internet service provider.[169]

---

163 "Federal law dated 01.05.2019 № 90-FZ "On amendments to the Federal law "On communications" and the Federal law "On information, information technologies and information protection"." *Internet Governance Project.* Available at: https://www.internetgovernance.org/wp-content/uploads/Federal-law-FZ-90-Summary.pdf, (last accessed on June 10, 2021).

164 Budnitsky, Stanislav. (2020). "Toward a Cultural Framework of Internet Governance: Russia's Great Power Identity and the Quest for a Multipolar Digital Order." *CARGC Papers*. 13.

165 *Ibid*.

166 Sleinan, Julett. (2021). "Experts Concerned About Growing Censorship in Russia." *Organized Crime and Corruption Reporting Project.* Available at: https://www.occrp.org/en/daily/14074-experts-concerned-about-growing-censorship-in-russia, (last accessed on May 24, 2021).

167 *Ibid*.

168 *Ibid.*

169 "Russia: Growing Internet Isolation, Control, Censorship." (2020). *HRW.* Available at: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship#:~:text=Russian%20internet%20users.-,The%20Sovereign%20Internet%20Law,state's%20control%20over%20internet%20infrastructure, (last accessed on June 7, 2021).

In November 2019, Putin's regime introduced further regulations that create the legal structure for the state organisation and control of the internet within Russian borders.[170] However, the technological requirements to enforce these changes would require assistance from other countries. Furthermore, to successfully assert its goals of digital sovereignty, Russia may benefit from aligning with China – which has similar goals to Russia. [171] While the practical aspects of enacting these regulations will prove complex, there is a high likelihood that this new set of laws will hasten the splintering of the global internet.[172]

Russia's goals can be essentialised into the following three parts:

i. creating effective surveillance mechanisms for the internet within its territory,

ii. the state acquiring status of a key regulator of Russian internet, and

iii. the expansion of the state-centric internet model internationally.[173]

These new amendments reflect Russia's continued move to an isolated and state-governed internet. State authority will have the ability to regulate the internet within borders better. Furthermore, state authority will use a kill switch or a mechanism that can shut down a mass of the Russian internet.[174] While the justifications for this kill-switch are under the more expansive scope of protecting sovereignty – there are worrying elements. The free-flowing and open nature of the internet ensures freedom of communication and access, whereas a kill-switch would be an "assault on freedom of expression."[175] A kill-switch supports a heavily censored and isolationist policy.[176] Needless to say that a 'kill-switch' policy will have a disproportionate impact on freedom of speech and expression and human rights.

Perhaps, the most interesting of these amendments is Russia's marked attempt at achieving independence from the ICANN system through its DNS.[177] If successfully executed, this would be a first. No other country to date has been able to establish its national DNS system. Consequentially, it is difficult to predict precisely how this would work in harmony with the existing system. This national DNS would potentially isolate Russian websites from the global DNS while simultaneously disallowing Russia from accessing the global DNS.[178] It may also

---

170 Epifanova, Alena. (2020). "Deciphering Russia's "Sovereign Internet Law."" DGAP Analysis 2, 11 p. Available at https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf, (last accessed on June 14, 2021).

171 *Ibid.*

172 *Ibid.*

173 *Ibid.*

174 *Ibid.*

175 "Russia's Assault on Freedom of Expression." (2017). *HRW.* Available at: https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression, (last accessed on June 7, 2021.)

176 Doffman, Zak. (2019). "Putin Now Has Russia's Internet Kill Switch to Stop U.S. Cyberattacks." Available at: https://www.forbes.com/sites/zakdoffman/2019/10/28/putin-now-has-russias-internet-kill-switch-to-stop-us-cyberattacks/?sh=6562fc2c31b2, (last accessed on June 10, 2021).

177 Epifanova, Alena. (2020). "Deciphering Russia's "Sovereign Internet Law."" DGAP Analysis 2, 11 p. Available at https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf, (last accessed on June 14, 2021).

178 *Ibid.*

be prudent for the broader ICANN community to weigh in at the national legislation enacted by Russia and its potential impact on the technical governance of the internet.[179]

3.3 EU/UK

Given the time this paper was written and ongoing Brexit negotiations, both the European Union (EU) and the United Kingdom will be analysed in one section. Some have postulated that the European formulation of sovereignty is independent of external threats of US tech giants, data leaks and others. However, others suggest discussions of digital sovereignty and privacy in Europe became more prominent following the events post-Snowden.[180] In light of the 2013 leak – freedom, privacy, and trust became a hot-button issue when discussing data, the cloud and computing.[181] While the Snowden leak was primarily concerned with the role of intelligence agencies, it brought to the foreground broader questions of data security, protection and privacy. Today, the digital landscape has become a cause of concern and insecurity for the Member States of the EU. Remarkably, there are concerns over citizens, businesses, and states losing agency over data, ability to innovate, and capacity to impact legislation.[182]

The GDPR applies to all within the EU in 2018 and replaced the prior Data Protection Directive of 1995. [183] The GDPR has status as a regulation, so it is applicable for all EU members. This is markedly different to the previous Data Protection Directive of 1995, which as an EU directive, bound members only to the desired outcome but not specific means to achieve the outcome. Prima facie, the GDPR facilitates extraterritorial jurisdiction. Meaning, the GDPR reaches beyond just the borders of the EU. If personal data is processed under the context of a controller or processor's organisation in the EU – it does not matter if the data is being processed in an independent country as it is within the context of the EU-based controller.[184] The GDPR applies to organisations within the EU and personal data being processed about the EU with territorial jurisdiction. Additionally, it applies to organisations that are not established

---

179 Veni Markovski and Alexey Trepykhalin, Country Focus Report: Russian Federation Internet-Related Laws and United Nations Deliberations, ICANN (2021), pg.3, available at: https://www.icann.org/en/system/files/files/ge-006-19jan21-en.pdf, (last accessed on June 14, 2021).

180 Hohmann, Mirko. (2014). "Technological Sovereignty: Missing the Point?" *Global Public Policy Institute.* Available at: https://www.gppi.net/2014/11/24/technological-sovereignty-missing-the-point, (last accessed on June 2, 2021).

181 Hoboken, Joris and Rubinstein, Ira. (2014). "Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era." *66 ME L. Rev. 487.* Available at: https://digitalcommons.mainelaw.maine.edu/cgi/viewcontent.cgi?article=1092&context=mlr, 488, (last accessed on June 10, 2021).

182 "Digital Sovereignty for Europe." (2020). *EPRS.* Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf, (last accessed on May 28, 2021).

183 Gaeta, Maria. "Hard Law and Soft Law on Data Protection: What A DPO should know to better perform his or her tasks." Available at: http://www.ejplt.tatodpr.eu/Fascicolo/article_html?ida=107, (last accessed on May 29, 2021).

184 "The Extra-Territorial Reach of EU Data Protection Law." (2019). Available at: https://www.sidley.com/en/insights/publications/2019/07/the-extra-territorial-reach-of-eu-data-protection-law, (last accessed on May 29, 2021).

in the EU, but process personal data related to offering goods or services in the EU or monitoring the behaviour of individuals within the EU. [185]

However, what is of particular interest is the language and framing of these approaches to digital sovereignty and governance. President of the European Commission, Ursula von der Leyden, made the agenda of prioritising technical sovereignty key. However, as previously noted, the definitions of digital sovereignty, technical sovereignty, and data sovereignty have been speculated upon and heavily contested. [186] Thus, there is little in the way of specificity and clarity as to what this meant. However, by March of 2020, the European Commission had set out new legislation to address the growth and proliferation of artificial intelligence, sellers in crucial places, and data regulation.[187] Furthermore, in the context of digital sovereignty, digital sovereignty here can be defined as "Europe's ability to act independently in the digital world." [188] While data sovereignty has not been referred to as a direct focus on the EU's approach to the digital space, digital and technological sovereignty has been highlighted.[189]

The Proposal for a Regulation on European data governance or the Data Governance Act is the first among many measures announced in 2020 by the EU to manage data. The purpose of this act is to bolster access to data through trust-increasing measures with data intermediaries and fortifying data-sharing mechanisms in the EU.[190] Data sovereignty within the EU and across member states is regulated by EU legislation.

The EU approach to data sovereignty and internet governance is value and human-rights based, focusing on EU norms of ethics and privacy. The EU addresses these matters with a focus on protecting privacy, protecting its citizens outside its jurisdiction and propagating the right to be forgotten.[191] Europe has used soft laws, multi-stakeholder directives, and other forums that have developed its digital procedures and practices. [192] Among these soft practices was the Data Protection Directive of 1995. However, these policies lack effective ways to assess and address harm or criminal behaviour.

---

185 Wimmer Kurt, CIPP/E, CIPP/US, Maldoff, Gabe, and Lee, Diana. (2020). "Comparison: Indian Personal Data Protection Bill 2019 vs. GDPR." *Iapp.* Available at: https://iapp.org/media/pdf/resource_center/india_pdpb2019_vs_gdpr_iapp_chart.pdf.

186 The European Union And the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World? Atlantic Council, n.d.

187 *Ibid.*

188 "Digital Sovereignty for Europe." (2020). *EPRS.* Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf, (last accessed on May 28, 2021).

189 *Ibid.*

190 "Proposal for a Regulation on European data governance (Data Governance Act)." Available at: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-data-governance-data-governance-act, (last accessed on June 3, 2021).

191 "European Digital Infrastructure and Data Sovereignty A Policy Perspective." Available at: https://www.eitdigital.eu/fileadmin/files/2020/publications/data-sovereignty/EIT-Digital-Data-Sovereignty-Summary-Report.pdf, (last accessed on June 14, 2021).

192 Hobbs, Carla. (2020). "Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry." *European Council on Foreign Relations.* Available at: https://ecfr.eu/wp-content/uploads/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf, (last accessed on June 14, 2021).

The EU has primarily centred its attempts at digital sovereignty around its ability to protect its citizens from external threats. We also cannot discount the impact of tech giants such as Facebook, Google, and Amazon. The most recent piece of proposed legislation to address these impacts is the EU's Digital Services Act (DSA). DSA is the European Commission's most recent effort at regulating tech companies. DSA is trying to regulate online intermediaries and platforms. It is meant to address a need that the current E-Commerce Directive has failed to address.[193] The European Commission website focuses on rules that are in cohesion with European values and norms, focusing on citizens' rights.[194]

3.4 USA

The US does not currently have general data privacy laws at the federal level.[195] Instead, American privacy laws are context and sector specific. US privacy laws are based on understandings of individual control when regulating data collection.[196] The sectoral system limits aspects of governance and creates unique governing frameworks. Regulators like the Federal Trade Commission (FTC) assist with regulating the internet – though it is limited in powers. [197]

The first of its kind - The US Privacy Act of 1974 was passed by Congress and protected the rights of citizens while restricting the collection and usage of data. This was the first piece of legislation of its kind that closely mirrors the concerns of today about data.[198] In the health sector, passed in 1996, the Health Insurance and Portability Act (HIPAA) was innovative in regulating health insurance. As part of HIPAA, the Secretary of the US Department of Health and Human Services (HHS) had to develop specific regulations detailing how to protect health information. HHS published the Privacy Rule and the Security Rule. The Privacy Rule details the standards of protection for health information, while the Security Rule establishes the security standards for protecting health information stored or transferred via electronic form.[199]

As previously mentioned, the FTC has some role in regulating the internet. The powers vested in the FTC can bring a charge against any companies engaged in "unfair or deceptive practices."[200] It did so in its 2012 case against Facebook. The FTC brought an eight-count

---

193 "The Digital Services Act package." Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package, (last accessed on June 3, 2021).

194 "The Digital Services Act: Ensuring a safe and accountable online environment." Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en#new-rules-in-a-nutshell, (last accessed on June 3, 2021).

195 Mooy, Michelle De. (2017). "Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data." Available at: https://cdt.org/wp-content/uploads/2017/04/Rethinking-Privacy_2017_final.pdf, (last accessed on June 14, 2021).

196 *Ibid.*

197 *Ibid.*

198 *Privacy Act of 1974.* Available at: https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20of%201974,of%20records%20by%20federal%20agencies.

199 U.S. Department of Health & Human Services. "Summary of the HIPAA Security Rule." Available at: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

200 FTC. (2019). "A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority." Available at: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, (last accessed on June 14, 2021).

complaint against Facebook, on the grounds that it had violated the trust of users through deceptive and poor privacy practices.[201] While the US lacks federal-level consumer data privacy law, many states do have new privacy acts. The California Consumer Privacy Act (CCPA), Massachusetts Data Privacy Law, New York Privacy Law, Hawaii Consumer Privacy Protection Act, Maryland Online Protection Act, North Dakota.

Foremost, when analysing US internet governance, there are many ongoing debates about whether the US has internet superiority or dominance. The Internet Assigned Numbers Authority (IANA) are technical arrangements that ensure that the internet works. The US government wished to privatise the IANA functions by the year 2000. However, when the government exceeded its deadline, the National Telecommunications and Information Administration (NTIA) assigned these functions to the Internet Corporation for Assigned Names and Numbers (ICANN). Following this, perception dictated that the US government controlled the internet.[202] This idea that the US government controls internet governance has had many lead-on effects, including the emergence of diverging governance paradigms.

Another legislation worth note is the CLOUD Act introduced in the House *of Congress* in 2018.[203] The CLOUD Act is an update of the 1986 Stored Communications Act (SCA).

The CLOUD Act was enacted to better the practices for both foreign and US investigators in gaining access to electronic information that service providers have.[204]

The bill amends national criminal law to detail electronic communication services (ECS) or remote computing service providers (RCS) must:

> "must comply with existing requirements to preserve, backup, or disclose the contents of an electronic communication or noncontent records or information about a customer or subscriber, regardless of whether the communication or record is located within or outside the United States" [205]

The ECS or RCS providers are empowered to challenge warrants to these contents in a few cases. Furthermore, the act allows the US and foreign governments to enter into agreements that govern data access. In order to be valid, executive agreements must comply with specific standards, including those imposed on the foreign government, which compels procedural privacy protections and minimisation procedures.[206] However, there are questions of how compliant with each foreign country or jurisdiction the US would be requesting. If the transfer

---

201 FTC. "Facebook Settles FTC Charges That it Deceived Consumers by Failing to Keep Privacy Promises." Available at: https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep, (last accessed on June 10, 2021).

202 Stifel, Megan. (2017). "Maintaining U.S. Leadership on Internet Governance." Available at: https://www.cfr.org/report/maintaining-us-leadership-internet-governance, (last accessed on June 11, 2021).

203 Congress.gov. "H.R.4943 - 115th Congress (2017-2018): CLOUD Act." February 6, 2018. https://www.congress.gov/bill/115th-congress/house-bill/4943.

204 *Purpose of the Cloud Act*. Available at: https://www.justice.gov/dag/page/file/1153466/download.

205 Congress.gov. "H.R.4943 - 115th Congress (2017-2018): CLOUD Act."

206 *Ibid.*

of data conflicts with an individual country's data protection laws, whether the US could attain foreign jurisdiction data remains in question.

Conclusion:

The aforementioned cases demonstrate a few aspects of internet governance for each of the above countries, which can be extrapolated to broader understandings of their governance methods. Countries privilege certain norms over the other and it is often these core values which sit at the root of governance policies.

These varying governance models can inform policy suggestions through an evaluation of the benefits and drawbacks of their respective policies. Things to be wary of include the following:

- Trends toward Russian and Chinese internet governance policy heavily focused upon continued isolationist methods and increasing Government's ability to censor the internet.
- The EU's GDPR as the only established large piece of legislation has created avenues for discussion. While it has been successful in some senses it has been unsuccessful in impacting large scale change.
- US internet governance is incredibly decentralised, and it is a notable example as it is sector specific. These examples are better contextualised the digital ecosystem.

The next chapter will evaluate India and provide essential considerations and feedback on the current systems to suggest the future system.

4. India

Introduction:

Data sovereignty in India has assumed significance over the past few years and become more significant in public discourse. Data sovereignty is increasingly understood as a non-negotiable in setting India's data agenda, and data governance proposals including but not limited to the Personal Data Protection Bill, the Draft National E-Commerce Policy and the Non-Personal Data Governance Framework suggest as much.[207] At present, India has established a digital sovereignty vision which includes the following three critical elements (i) an emphasis on data as a keystone in economic growth and development, (ii) disallowing unabated cross-border data flows, and (iii) the use of/access to data when there are security threats.[208] Moreover, as will be substantiated below there is a clear emphasis on the need for data localisation. Data localisation can often become a means to assert sovereignty. Localisation is tied to self-determination and independence.

Amongst all the regulatory developments that are ongoing in India, of particular importance are – (i) The Personal Data Protection Bill and (ii) The Non-Personal Data Governance

[207] Kovacs, A., Ranganathan, N. (2019). Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India. Data Governance Network Working Paper 03.

[208] https://www.orfonline.org/expert-speak/sovereignty-datafied-world-framework-indian-diplomacy/.

Framework (NPD). These legislations do establish frameworks for the governance and protection of data. These frameworks are also pushing for data localisation. [209] With the proposed legislation, the State is empowered to intervene and access information. Arguably, this would mean that the State would be able to exercise control over the internet governance and digital sovereignty agenda. The model of governance proposed in India's bills is akin to the sovereign-difference ideal discussed in the preceding sections.

In 2015, during the BRICS summit in Russia, India endorsed its support towards a multistakeholder model and consequently shifted from its previous preference of multilateral process of internet governance.[210] The Minister for Communications and Information Technology stated that barring national security matters, where governments would have a supreme right of control, India believe that the internet must be managed through a multistakeholder process. The Minister thus stated, "Every Indian must have the capacity to participate in global decision-making on how we manage this common resource – and so must every global citizen."[211]

4.1 Framing Data Sovereignty in India (in Dialogue and Discourse)

Public discourse in this scenario and the words of key public figures and institutions illustrate how data and digital sovereignty have been framed in the Indian context. Sovereignty in data is often presented as a form of empowerment and self-determination for states. This notion is the repurposing of traditional conventions of sovereignty in the digital context; however, this sovereignty looks very different in the digital sphere. Elaborated below are examples of how critical public figures and institutions have engaged with this issue in India:

- **Department of Telecommunications (DoT):** The DoT published the "National Digital Communications Policy of 2018." The third 'Mission' of the policy was, "To secure the interests of citizens and safeguard the digital sovereignty of India with a focus on ensuring individual autonomy and choice, data ownership, privacy and security; while recognizing data as a crucial economic resource."[212] It serves to represent the autonomy of Indians.
- **Ministry of Communications and Information Technology:** In 2020, Ravi Shankar Prasad, the Minister of Communications, Electronics & Information Technology and Law & Justice, said, "We shall never compromise on data sovereignty of India. India being an important digital power, our data sovereignty will be very very important. And we shall ensure that we are never made to do any compromise, nor we will do that (compromise)."[213]

---

209 The Personal Data Protection Bill, Chapter VII, addresses the restriction on transferring personal data outside India. Section 33 focuses on the restriction of processing sensitive personal data and critical personal data outside India. This section outlines limits on data flow and stipulates that critical personal data is stored in India.

210 Brotman, Stuart, N. (2015). "Multistakeholder Internet governance: A pathway completed, the road ahead." *Centre for Technology Innovation at Brookings*. Available at: https://www.brookings.edu/wp-content/uploads/2016/06/multistakeholder-1.pdf, (last accessed on June 11, 2021).

211 *Ibid.*

212 Department of Telecommunications, *National Digital Communications Policy 2018.* 2018, 5.

213 Press Trust of India. (2020). "India 'important digital power' won't compromise on data sovereignty: Ravi Shankar Prasad," *Economic Times.* Available at: https://economictimes.indiatimes.com/tech/ites/india-

In March 2021, the Minister stated before the Rajya Sabha that the "imperialism of internet" by a few businesses would not be allowed.[214] In late May of 2021, Ravi Shankar Prasad again reiterated the focus on India's digital sovereignty and said, "we will not compromise on the issue of India's digital sovereignty." [215]

- **Department for Promotion of Industry and Internal Trade:** In February of 2019, the Department for Promotion of Industry and Internal Trade (DPIIT) released the Draft National E-Commerce Policy. In the document, data is said to "warrants treating it at par on which a country would have sovereign right."[216] It also reiterates that India and its citizens "have a sovereign right to their data."[217]
- **Mukesh Ambani (Chairman and MD of Reliance Industries):** Reliance Chairman Ambani has openly endorsed data localisation as a way to avoid data colonisation. In 2019, he demonstrated support for data localisation, asserting that data produced by India should be controlled and owned by Indians.[218] This push for ownership is an attempt at exercising data ownership and promoting Indian data sovereignty.

In the judicial sector, the benchmark ruling of the Puttaswamy Judgement[219] created a helpful framework to understand the stance on privacy and the importance of users owning their data. India has subscribed to a sovereign-difference ideal for the governance of its internet and data. On the issue of data sovereignty in the *Swami Ramdev & Anr. vs Facebook, Inc. & Ors*,[220] the High Court of Delhi court ruled that Indian courts could provide takedown orders for global platforms (including Facebook) with illegal content when content is either uploaded from India or the information or data is located in India. An appeal met this ruling on the grounds of the ruling violating national sovereignty and international comity.[221] Union Commerce and Industry & Railways Minister, Piyush Goyal, has also publicly recognised data as a sovereign

important-digital-power-wont-compromise-on-data-sovereignty-prasad/articleshow/76840586.cms, (last accessed on June 14, 2021).

214 Press Trust of India. (2021). "Any attempt to create 'imperialism of internet' by few companies unacceptable: Ravi Shankar Prasad," *Financial Express.*

215 Sharma, Rajat. (2021). "There can be no compromise on India's digital sovereignty: Ravi Shankar Prasad." Available at: https://www.indiatvnews.com/news/india/there-can-be-no-compromise-on-india-s-digital-sovereignty-ravi-shankar-prasad-aaj-ki-baat-rajat-sharma-opinion-blog-707857, (last accessed on June 10, 2021).

216 Draft National e-Commerce Policy, 2019. Available at: https://dipp.gov.in/whats-new/draft-national-e-commerce-policy-stakeholder-comments.

217 *Ibid.*

218 Press Trust of India. (2019). "India's data must be controlled by Indians: Mukesh Ambani." *Mint.* Available at: https://www.livemint.com/Companies/QMZDxbCufK3O2dJE4xccyI/Indias-data-must-be-controlled-by-Indians-not-by-global-co.html, (last accessed on June 14, 2021).

219 JUSTICE K S PUTTASWAMY (RETD.), AND ANR. VS UNION OF INDIA AND ORS [2017] WRIT PETITION NO 494 OF 2012. Available at: https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

220 SWAMI *RAMDEV & ANR. versus FACEBOOK, INC. & ORS [2019]*. Available at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/01/Ramdev-v.-Facebook-Delhi-HC.pd (last accessed on June 10, 2021).

221 Tripathi, Karan. (2020). "'Why Are you Aggrieved By Global Injunction Order?': Delhi HC Asks Facebook In Baba Ramdev's Case," *LiveLaw.in*.(last accessed on June 2, 2021).

asset. Goyal has maintained the idea that countries are entitled to the sovereign right to the data they generate. [222]

These statements are all significant as they are the views of experts and key stakeholders within the space.

4.1.1 Data Colonialism and Imperialism

Part of the framing dialogue is that data sovereignty is a way to fight data colonisation/data imperialism. Data sovereignty is antithetical conceptually to data colonisation.[223]Data colonialism is leveraged as the stark binary opposite to data sovereignty, where a few foreign tech companies control large amounts of data.[224] Nandan Nilekani, co-founder of Infosys, publicly recognised the threat of data colonisation, though Nilekani has not specified an agenda on data localisation.[225] However, this acknowledgement implies the strength of the notion of data colonialism in the public consciousness.

4.1.2 Digital Nationalism

We can understand that part of the agenda and framing is that protecting digital sovereignty and security means aligning digital content access with political interests. Chinese apps were blocked in 2020 to ensure sovereignty and security.[226] Digital nationalism is a concept that aligns digital actions with the political status quo. Digital nationalism, while seemingly harmless, can be harmful. In and of itself, pushes for data localisation and data sovereignty are not worrying. However, trends towards an isolationist internet, with internet shutdowns, data localisation and firewalls, may be a cause for concern.[227]

Digital nationalism is separate from digital sovereignty or sovereign-difference ideals. It has a more aggressive approach to territorialising the internet.[228] Digital nationalism is evident in laws that heavily restrict digital content and access. For example, China's model of the internet

---

222 Ranganathan, Nayantara. (2019). "The seduction of data sovereignty in India." *Hindustan Times.* Available at: https://www.hindustantimes.com/analysis/the-seduction-of-data-sovereignty-in-india/story-iOS8cVKxstIIgJLy47Iy0J.html, (last accessed on June 9, 2021).

223 Kovacs, A., Ranganathan, N. (2019). Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India. Data Governance Network Working Paper 03.

224 *Ibid.*

225 Pramanik, Ayan. (2017). "Need policy against data colonisation: Nandan Nilekani." *Business Standard*. Available at: https://www.business-standard.com/article/technology/need-policy-against-data-colonisation-nandan-nilekani-117080900007_1.html, (last accessed on June 13, 2021.)

226 Press Trust of India. (2020). "India 'important digital power' won't compromise on data sovereignty: Ravi Shankar Prasad," *Economic Times.* Available at: https://economictimes.indiatimes.com/tech/ites/india-important-digital-power-wont-compromise-on-data-sovereignty-prasad/articleshow/76840586.cms, (last accessed on June 14, 2021).

227 Kapur, Akash. (2019). "The Rising Threat of Digital Nationalism." *Wallstreet Journal.* Available at: https://www.wsj.com/articles/the-rising-threat-of-digital-nationalism-11572620577, (last accessed on June 13, 2021).

228 *Ibid.*

is more clearly a brand of digital nationalism.[229] The most helpful way to avoid digital nationalism is to encourage transparency, openness, and equality.

4.1.3 Data Localisation

There have been increasing pushes for data localisation and broad localisation – this could also be noted as the novel concept of data nationalism. Continued promotion of data localisation to protect the sovereign asset of data does not hold water. First, data cannot be restricted to a single state. Localising data cannot be fully achieved in a country that wishes to participate in the global internet. Data localisation presently exists in sector-specific policies, for example, in payment systems. Data localisation in India formally began in 2018 when the Reserve Bank of India directed all companies to store data related to payment systems in India.[230]

Data localisation would realign data flows to affect power and serve as a representation of state sovereignty.[231] Data localisation is the implementation of varying policy tools to limit data flow through and specify its physical storage and processing within a given territory.[232]

Data localisation has become increasingly part of the policy dialogue in India.[233] Data localisation has been stated to fulfil the following four key objectives:

- better access to personal data for law enforcement
- supporting development and economic growth
- preventing foreign surveillance
- and creating a more efficient ecosystem for the implementation of local data protection laws.[234]

Nevertheless, data localisation is not the solution for all the objectives mentioned above. Data localisation and data access are not the same.[235] Data localisation entails the act of restricting data flows and limiting where it is stored and processed. Even if data is heavily restricted to Indian territory, this does not guarantee access for parties or government institutions that seek it.

---

229 *Ibid.*

230 Basu, Arindajit. (2020). "The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam." Available at: https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/, (last accessed on June 14, 2021).

231 Kovacs, A., Ranganathan, N. (2019). Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India. Data Governance Network Working Paper 03.

232 Anirudh Burman and Upsana Sharma. (2021). "How Would Data Localisation Benefit India?" *Carnegie India.* Available at: https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291, (last accessed on June 14, 2021.)

233 *Ibid.*

234 *Ibid.*

235 *Ibid.*

4.2 Policy

In the interest of brevity, we will not describe all aspects of the relevant policies. Instead, we will focus on the areas of concern and suggest improvement wherever possible. The highlighted areas are the ones which require the most attention as lack of clarity in these categories could be detrimental.

4.2.1 Personal Data Protection Bill

The Personal Data Protection Bill is meant to control the collection, processing, storage, usage, transfer, protection, and disclosure of personal data.

The bill requires the localisation of "sensitive personal data" within India. This bill also has been referred to as the first economy-wide data localisation framework.[236] "The Personal Data Protection Bill, 2019" (PDB) creates a framework for how data should be processed, stored while providing insight into people's rights regarding their personal information. The bill is meant to provide a paradigm shift in Indian data governance and protection, currently governed by the *Information Technology Act, 2000*.[237] The bill also suggests creating a new regulatory authority, the Data Protection Authority (DPA), to ensure the enforcement of this law. The bill comments that "sensitive personal data" be stored within India and "critical personal data" must remain within India.[238]

In the bill, personal data is "data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling."[239] Sensitive personal data is any personal data that can reveal, be connected to or comprise: financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation, or any data categorised as sensitive per section 15 of the bill.[240] Section 15 specifically states that personal data is classified as sensitive personal data when the Central Government and Authority deem categories as such in these instances:

- if risk of harm that could be caused is significant by the processing of the data
- if there is an expectation of confidentiality attached to the data

---

236 *Ibid.*

237 Kittane, P., Charles, I., S., Kamath, A., Gokhale, G. (2021). "Privacy and Data Protection – India Wrap 2020." Available at: https://www.natlawreview.com/article/privacy-and-data-protection-india-wrap-2020, (last accessed on June 14, 2021).

238 Anirudh, Burman and Suyash, Rai. (2020). "What is India's Sweeping Personal Data Protection Bill?" *Carnegie India.* Available at: https://carnegieindia.org/2020/03/09/what-is-in-india-s-sweeping-personal-data-protection-bill-pub-80985, (last accessed on June 14, 2021.)

239 Personal Data Protection Bill, 2019. http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

240 *Ibid.*

- if a distinct group of data principals would suffer significantly by the processing of the category of data
- where the suitability of protection by regular provisions applies to personal data.[241]

The processing of critical personal data and sensitive personal data outside of India is prohibited under Chapter VII of the PDB. This restriction of data flows and their processing is an example of data localisation.

Data fiduciaries have been named as those in charge of enforcing this new regulation – and will have responsibilities that also include performing data audits and selecting data protection officers.[242] The bill, however, does not address how businesses will be compensated for losses incurred by these new measures, as it is speculated that there could be damaging long-term consequences for economic growth in India. However, Chapter VIII, Exemptions, of the PDB, provides ambiguous terms for exempting any Central Government agency from all other directives of the Act.[243]

4.2.2 The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Recently, the government passed the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The Rules stipulate inter alia, that significant social media intermediaries are compelled to identify the first originator of information required by a court or order. These orders are passed to prevent, detect, investigate, prosecute, or punish a wrongdoing concerning India's sovereignty and integrity, security, foreign states' relations, etc. All mentions of sovereignty within the Rules refer to potential threats which harm the broad sovereignty of India. These mentions do not pertain explicitly to data sovereignty.[244] However, while there is no explicit mention of data sovereignty, the demand to comply with the new Rules for foreign social media intermediaries in India is an exercise of sovereignty.

4.2.3 Non-Personal Data Governance Framework

Following the introduction of the PDB, the Committee proposed the Non-Personal Data (NPD) Framework in July 2020. The NPD framework addresses many novel ideas on non-personal data and attempts to provide definitional clarity on which rights and privileges are guaranteed for such data. NPD also details consent requirements for anonymising data, the sensitivity of non-personal data, and defining intent for data sharing.[245] The NPD framework applies to all data that is not personally under the PDB or does not have any personally identifiable information. It also notes that non-personal data will remain governed by NPD framework if it remains non-personal, but when data that is anonymised is re-identified, it will be regulated by

---

241 *Ibid.*
242 *Ibid.*
243 *Ibid.*
244 Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021.
245 Data Guidance. (2020). "India: MeitY releases report on non-personal data governance framework and seeks feedback." *Data Guidance*. Available at: https://www.dataguidance.com/news/india-meity-releases-report-non-personal-data, (last accessed on June 14, 2021.)

PDB. The revised report also revises the scope of requirement requiring organisations to share anonymised datasets.

The NPD also provides further insight into what is considered "data business." The obligatory data sharing has been amended in the revised framework. An original requirement to share data for economic purposes with other companies has been removed.[246]

NPD defines non-personal data as "all data that is not personal data". The NPD also defines the concept of "sensitive" non-personal data. The Non-Personal Data Governance Framework makes specific recommendations for the regulation of Non-Personal Data in India.[247]

The Non-Personal Data Governance Framework highlights three categories of Non-Personal Data, namely:

- public data, such as public health information;
- community non-personal data, such as datasets containing user-information gathered by private players; and
- private non-personal data, such as imputed insights relating to algorithms.[248]

However, despite these envisioned distinctions, datasets cannot be this bifurcated along the lines of personal and non-personal. One of the significant issues of the NPD is its false dichotomy that personal data ought to be protected while non-personal data should not be allotted the same protections.[249]

The NPD does not create appropriate mechanisms for accountability.

4.2.4 The Draft National E-Commerce Policy

The Indian government has been mulling a draft e-commerce policy for the past two years. While the government released a Draft National E-Commerce Policy in 2019 with a view to provide a framework for regulating the rapidly growing digital economy. The document sought to provide a framework allowing India to benefit from the digitisation of the national and global economy. Among other things, the draft policy opined that a country's data is best understood as a national asset that the government holds in trust. It states that Indians have a sovereign entitlement to their data, as the draft considers data 'about' an individual as that 'individual's data'. This is considered valid even after data has been anonymized. The draft also suggested

246 Kurth, Hunton., Andrews. (2021). "India Releases Revised Non-Personal Data Framework." Available at: https://www.natlawreview.com/article/india-releases-revised-non-personal-data-framework, (last accessed on June 14, 2021.)

247 Report by the Committee of Experts on Non-Personal Data Governance Framework.

248 Marda, Vidushi. (2020). "Non-personal data: the case of the Indian Data Protection Bil, Definitions and Assumptions." Available at: https://www.adalovelaceinstitute.org/blog/non-personal-data-indian-data-protection-bill/, (last accessed on June 14, 2021).

249 Michèle Finck and Frank Pallas. (2020). "They who must not be identified—distinguishing personal from non-personal data under the GDPR." *International Data Privacy Law*, Volume 10, Issue 1Pages 11–36, Available at: https://doi.org/10.1093/idpl/ipz026.

that cross-border data flows should be restricted. This suggestion was premised on the assumption that to be successful, Indian business entities must be able to access Indian data. In this scenario, if other countries can access the data generated within India it would diminish the value of Indian digital products. The draft also suggested localising physical facilities for computing and processing data.[250] Overall, this draft promoted localisation efforts by restricting cross-border data flows and physically altering where the computing and processing of data occurs. When this draft was released in 2019, several foreign e-commerce companies raised concerns over some points in draft pertaining to data.[251]

According to recent media reports, the new policy that the government is presently working on is anticipated to have regulations preventing misuse of data. The draft policy proposes safeguards that may include restricting cross-border flow of the data pertaining to Indians and the transactions taking place in the country. It may also recommend carrying out audits of the storage locations of these entities.[252] The government is expected to carry out stakeholder consultations over the proposed draft.[253]

4.3 Comments and Considerations

Data sovereignty claims sometimes construct data as a resource to be used to bolster economic enrichment.[254] Large parts of the Indian population have only recently had access to the internet, while large swathes still do not.[255] Internet usership has exploded in the last few years. In 2007, the number of internet users was 134 million. By 2017, this number was 422 million.[256] According to the Telecom Regulatory Authority of India, the active internet user population was 749 million by June 2020.[257] By 2025, this number is predicted to reach 900 million.[258]

---

250 Draft National e-Commerce Policy, 2019. Available at: https://dipp.gov.in/whats-new/draft-national-e-commerce-policy-stakeholder-comments.

251 "DPIIT 'definitely' working on new e-commerce policy: Govt official." (2021). *Business Standard* (online), available at: https://www.business-standard.com/article/economy-policy/dpiit-definitely-working-on-new-e-commerce-policy-govt-official-121020500854_1.html, (last accessed on June 14, 2021).

252 "Draft e-commerce policy: Govt mulls new probe body, data audits," (2020). *Financial Express* (online), available at: https://www.financialexpress.com/economy/draft-e-commerce-policy-govt-mulls-new-probe-body-data-audits/2145985/, (last accessed Jun 14, 2021).

253 Kalra, Aditya. (2021). "India's draft e-commerce policy calls for equal treatment of sellers." *Reuters* (online). Available at: https://www.reuters.com/article/us-india-ecommerce-policy-idUSKBN2B50DT, (last accessed on June 14, 2021).

254 Kovacs, A., Ranganathan, N. (2019). Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India. Data Governance Network Working Paper 03.

255 *Ibid.*

256 Iyengar, Rishi. (2018). "The Future of the Internet Is Indian." *CNN Business.* Available at: https://edition.cnn.com/interactive/2018/11/business/internet-usage-india-future/, (last accessed on June 14, 2021).

257 Telecom Regulatory Authority of India. "The Indian Telecom Services Performances Indicator April – June 2020." TRAI: New Delhi, India. Available at: https://trai.gov.in/sites/default/files/Report_09112020_0.pdf (last accessed on June 10, 2021).

258 Press Trust of India. "Active internet users likely to reach 900 mn by 2025: IAMAI." *Business Standard.* Available at: https://www.business-standard.com/article/technology/active-internet-users-in-india-likely-to-reach-900-mn-by-2025-iamai-121060300710_1.html, (last accessed on June 12, 2021).

Sector-specific policies should be considered more closely. All data is not equal, and neither should its treatment be. The potential for harm caused by healthcare information being weaponised versus music streaming data is different.[259] Personal music browsing preferences cannot be used to the same degree of harm to discriminate against an individual. This dataset contains relatively benign information in comparison to health data. Whereas, if health information is leaked or misused, it can substantially harm an individual or community's interests. These distinctions between the sensitivity of information are frequently made in guidelines for assessing the severity of data breaches.[260]. The draft NPD was revised upon recommendations though its objectives and definitions remain unchanged from the initial report.[261] in early 2020, the Joint Parliamentary Committee requested public comments on the PDB.[262] In the absence of transparency and stakeholder consultation processes like these, there is a risk of losing stakeholder (consumer) trust and also minimising chances of improvement. Therefore, in order to ensure multistakeholder policy development process, it is recommended that policy-making should follow an open and transparent process.

The PDB does not ensure citizens' protection of rights or empowerment. Sections of the Personal Data Protection Bill, 2019 (Clause 35) provide the government with an avenue to access citizens' data under the claim of national security.[263] This undermines the purpose of the PDB and disempowers the individual.

Conclusion:

These bills and regulations symbolise a shift in the approach to data and information privacy in the Indian paradigm. Meanwhile, non-personal data as a separate ecosystem is perhaps more ambiguous than personal data. The NPD itself provides little in the way of clearing up such confusion. Part of this confusion is due to the blurry nature of the two personal and non-personal data categories.[264]

---

259 Dixon, P. (2017). "A Failure to "Do No Harm" – India's Aadhaar Biometric ID Program and its Inability to Protect Privacy in Relation to Measures in Europe and the U.S. *Health Technol*." 7(4): 539-567. Available at: https://link.springer.com/content/pdf/10.1007%2Fs12553-017-0202-6.pdf (last accessed on June 12, 2021).

260 *Guidelines 01/2021 on Examples Regarding Data Breach Notification.* European Data Protection Board, 2021. Available at: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.

261 "Revised Report by the Committee of Experts on Non-Personal Data Governance Framework." (2021). *Trilegal.* Available at: https://www.trilegal.com/index.php/publications/analysis/revised-report-by-the-committee-of-experts-on-non-personal-data-governance (last accessed on June 12, 2021).

262 Mandavia, Meghan. (2020). "Parliamentary panel invites comments on personal data protection bill." *The Economic Times.* Available at: https://economictimes.indiatimes.com/news/politics-and-nation/parliamentary-panel-invites-comments-on-personal-data-protection-bill/articleshow/73589688.cms?from=mdr, (last accessed on June 12, 2021).

263 Personal Data Protection Bill, 2019. http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf (last accessed on June 12, 2021).

264 Marda, Vidushi. (2020). "Non-personal data: the case of the Indian Data Protection Bil, Definitions and Assumptions." Available at: https://www.adalovelaceinstitute.org/blog/non-personal-data-indian-data-protection-bill/, (last accessed on June 14, 2021).

The NPD requires work to frame the issues surrounding non-personal data, as it does not highlight the dangers associated with the abuse of non-personal data. Both the NPD and PDB suggest the creation of respective authorities. These governance frameworks have their place and are promising for the future of the Indian internet governance paradigm but do still room for further clarity and definition to embolden the protection of individuals and communities.

Data sovereignty can be comprehended differently from how it is currently. Data sovereignty can apply beyond the state concept of data sovereignty and be extended to protect individual citizens. It can be understood as the rights of the sovereign citizen rather than the state where the state can protect it. Transparency and accountability are essential to further this objective.

5. Policy Recommendations

Evidently, the digital landscape has evolved tremendously over the past few decades, and countries across the globe are grappling with 'regulating' the seemingly 'unregulated' cyberspace. As has been discussed in detail throughout this paper, one of the key challenges is that the internet exists beyond the metes and bounds of traditional notions of sovereignty. And with most economies moving online on account of the pandemic, regulators across the world are grappling with vulnerabilities posed by an 'unregulated' internet including but not limited to cybercrime, domain name abuse, and propagation of fake news. Bearing in mind some of these challenges based on our research and analyses following are some recommendations for forward thinking on this subject:

1. Following the sovereign-difference ideal

Countries have the right to exercise legitimate authority within its own territory, including authority over data and data infrastructure in the territory, over the people and firms in the territory that use the data and infrastructure. [265] Through respecting the principle of comity and deferring to other states, not through compulsion but mutual respect – the digital sphere will be simpler to navigate. It is ineffective to operate under the assumption that all states will follow the same set of rules and laws, as the sovereign-difference ideal clarifies. As such, the sovereign-difference ideal views internet operating differently in different places according to local norms, customs, and rules.[266]

2. Focusing on the rights of the individual user

Concerning perceived threats of digital colonialism and threats to sovereignty, it is fundamental to remember that the individual user's rights should be treated with utmost importance. Therefore, ideas of digital sovereignty and data sovereignty should be reframed to focus on the individual. Individuals should be empowered to make informed decisions over their data. For this to be possible, individuals should have access to their data and avenues for recourse in cases where data is misused. However, to ensure that individuals are competently navigating the internet, it is important to ensure that they are educated about the risks lurking in the digital

[265] Woods, Andrew. (2018). "Litigating Data Sovereignty". Yale Law Journal, 328 - 406.
[266] *Ibid.*

space and the Indian government should undertake extensive digital awareness programs to facilitate this. Furthermore, the onus should be on entities seeking consent from the user to ensure that the language used is easy to understand and age as well as audience appropriate.

3. Creating a panel of experts to make decisions

Many aspects of policymaking in the digital space are obfuscated in a cloud of technical and practical ambiguity. Policymakers cannot be expected to learn all functional aspects of cloud technology, data localisation, cross-border data transfers and more. It would be most efficient and effective for a panel of experts from varying backgrounds to make decisions. This panel would include academics, policymakers, members of the private sector, and experts with technical expertise. For example, Japan has a panel of experts known as the Personal Information Protection Committee (PPC) responsible for enforcing its data protection legislation. [267] This commission is composed of a chairperson and eight commission members. The requirements for election to this committee include people who have knowledge and experience in: (i) the protection of and appropriate use of personal information, (ii) the protection of consumers, (iii) information processing technology, in administrative fields used in specific personal information, and (v) matters relating to private enterprises. This commission also includes a person recommended by six organisations: governors, mayors, presidents, and local councils.[268] It may be prudent to have a similar panel of experts under the Ministry of Electronics and Information Technology (MeitY) which is also the nodal ministry for internet governance issues to facilitate nuanced policymaking in this ever-evolving technological landscape.

4. Promote collaborative policymaking

Data pervades every aspect of modern-human life. Data does not exist in a vacuum and must be regulated with this knowledge. Narrowly focused institutions can create exclusionary policies when policies should instead allow for collaboration across sectors. A recent market study conducted by the Competition Commission of India in 2020 on the Indian Telecom Sector noted the need for comprehensive policy making approaches. The study noted how the telecom industry has transformed into an industry which collects large amounts of data, and there are potential risks that accompany this vast aggregation of data. It notes how regulation should be robust as the jurisdictional overlap between regulating bodies is not uncommon. [269] Thus, the best solution would be one that accounts for this and allows for inter - regulatory consultation in the decision-making process.

---

267 "Commission." PPC, Personal Information Protection Commission JAPAN. Available at: https://www.ppc.go.jp/en/aboutus/commission/, (last accessed on June 10, 2021).

268 *Ibid.*

269 *Market Study on the Telecom Sector In India – Key Findings and Observations.* New Delhi: Competition Commission of India, 2021. Available at: https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-Study-on-the-Telecom-Sector-In-India.pdf, (last accessed on June 10, 2021).

5. Allow public viewing, discussion, and commentary on policy

With its endorsement of the multistakeholder model of internet governance, India effectively announced to the global community that it believes in a bottom-up approach towards policy making. A truly multistakeholder approach requires accountability, transparency and open discourse between divergent views while formulating policies, bills, and regulations. Therefore, the public should be provided avenues for viewing, discussing and commenting on policy. Using a stakeholder model could prove highly germane. Stakeholder engagement with legislation and governance in the digital space has become increasingly popular. This can be attributed mainly to trends toward transparency and accountability.[270] Stakeholder consultation can ensure avenues for better discussion, management, and policy development. Without this consultation mechanism, policy development can become unbalanced. In order to ensure that India retains its commitment to multistakeholder model, it is imperative that legislations are formed through a stakeholder consultation process with every member of the society given an opportunity to put forth their points of view.

6. Policies should be sector-specific

Broad approaches to governance that do not address sector-specific needs can become problematic. For example, data protection frameworks that apply to healthcare and insurance do not have the same potential impact for harm as music streaming service data. These distinctions should be apparent through separate policies. When all data protection frameworks overlap on the concept of data alone, with distinctions being as simple as personal and non-personal, there is a lack.

7. Provide opportunities for long-term feedback

For the long-term success of policies, there should be chances for quarterly reviews of feedback submitted by the public. While policies can seem initially attractive, they can quickly become outdated with new technologies or only become impractical after implementation.

[270] Anderson, Vanessa., Burman, Baranaby., Foxwell, Roswell., and Wood, Iain. "Stakeholder Engagement in the Digital Age." IAIA Conferences, 2015.
Available at: https://conferences.iaia.org/2015/Final-Papers/Foxwell,%20Russell%20%20-%20Stakeholder%20Engagement%20in%20the%20Digital%20Age.pdf, (last accessed on June 10, 2021).

References

Anderson, Vanessa., Burman, Baranaby., Foxwell, Roswell., and Wood, Iain. "Stakeholder Engagement in the Digital Age." IAIA Conferences, 2015.

Available at: https://conferences.iaia.org/2015/Final-Papers/Foxwell,%20Russell%20%20-%20Stakeholder%20Engagement%20in%20the%20Digital%20Age.pdf, (last accessed on June 10, 2021).

Angwin, Julia, Larson, Jeff, Mattu, Surya, and Kirchner, Laura. (2016). "Machine Bias." *ProPublica.* Available at*:* https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, (last accessed on June 13, 2021).

Anirudh, Burman and Suyash, Rai. (2020). "What is India's Sweeping Personal Data Protection Bill?" *Carnegie India.* Available at: https://carnegieindia.org/2020/03/09/what-is-in-india-s-sweeping-personal-data-protection-bill-pub-80985, (last accessed on June 14, 2021.)

Anirudh Burman and Upsana Sharma. (2021). "How Would Data Localisation Benefit India?" *Carnegie India.* Available at: https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291, (last accessed on June 14, 2021.)

Baird, Zoë. (2002.) "Governing the Internet: Engaging Government, Business, and Nonprofits." *Foreign Affairs* 81, no. 6: 15-20. doi:10.2307/20033341.

Basu, Arindajit. (2020). "The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam." Available at: https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/, (last accessed on June 14, 2021).

Brotman, Stuart, N. (2015). "Multistakeholder Internet governance: A pathway completed, the road ahead." *Centre for Technology Innovation at Brookings*. Available at: https://www.brookings.edu/wp-content/uploads/2016/06/multistakeholder-1.pdf, (last accessed on June 11, 2021).

Budnitsky, Stanislav. (2020). "Toward a Cultural Framework of Internet Governance: Russia's Great Power Identity and the Quest for a Multipolar Digital Order." *CARGC Papers*. 13.

"Cambridge Analytica's Facebook Data Abuse Shouldn't Get Credit for Trump." (2018). *The Verge.* Available at: https://www.theverge.com/2018/3/20/17138854/cambridge-analytica-facebook-data-trump-campaign-psychographic-microtargeting, (last accessed on June 7, 2021).

Chatham House. (2016). *Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance: Research Volume Two Global Commission on Internet Governance.* Available at: https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202%20WEB.pdf. , (last accessed on June 12, 2021).

"Commission." PPC, Personal Information Protection Commission JAPAN. Available at: https://www.ppc.go.jp/en/aboutus/commission/, (last accessed on June 10, 2021).

Congress.gov. "H.R.4943 - 115th Congress (2017-2018): CLOUD Act."

Cramer, Benjamin W. (2018). "A Proposal to Adopt Data Discrimination Rather than Privacy as the Justification for Rolling Back Data Surveillance." *Journal of Information Policy* 8: 5-33. Accessed June 14, 2021. doi:10.5325/jinfopoli.8.2018.0005.

Dastin, Jeffrey. (2018). "Insight – Amazon scraps secret AI recruiting tool that showed bias against women." *Reuters.* Available at: https://in.reuters.com/article/amazon-com-jobs-automation/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idINKCN1MK0AH, (last accessed on June 14, 2021).

Data Guidance. (2020). "India: MeitY releases report on non-personal data governance framework and seeks feedback." *Data Guidance.* Available at: https://www.dataguidance.com/news/india-meity-releases-report-non-personal-data, (last accessed on June 14, 2021.)

Department of Telecommunications, *National Digital Communications Policy 2018.* 2018, 5.

"Digital Sovereignty for Europe." (2020). *EPRS.* Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf, (last accessed on May 28, 2021).

Dixon, P. (2017*).* "A Failure to "Do No Harm" – India's Aadhaar Biometric ID Program and its Inability to Protect Privacy in Relation to Measures in Europe and the U.S. *Health Technol*." 7(4): 539-567. Available at: https://link.springer.com/content/pdf/10.1007%2Fs12553-017-0202-6.pdf (last accessed on June 12, 2021).

Doffman, Zak. (2019). "Putin Now Has Russia's Internet Kill Switch to Stop U.S. Cyberattacks." Available at: https://www.forbes.com/sites/zakdoffman/2019/10/28/putin-now-has-russias-internet-kill-switch-to-stop-us-cyberattacks/?sh=6562fc2c31b2, (last accessed on June 10, 2021).

"DPIIT 'definitely' working on new e-commerce policy: Govt official." (2021). *Business Standard* (online), available at: https://www.business-standard.com/article/economy-policy/dpiit-definitely-working-on-new-e-commerce-policy-govt-official-121020500854_1.html, (last accessed on June 14, 2021).

Draft National e-Commerce Policy, 2019. Available at: https://dipp.gov.in/whats-new/draft-national-e-commerce-policy-stakeholder-comments.

"Draft e-commerce policy: Govt mulls new probe body, data audits," (2020). *Financial Express* (online), available at: https://www.financialexpress.com/economy/draft-e-commerce-policy-govt-mulls-new-probe-body-data-audits/2145985/, (last accessed Jun 14, 2021).

Epifanova, Alena. (2020). “Deciphering Russia’s “Sovereign Internet Law.”” DGAP Analysis 2, 11 p. Available at https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf, (last accessed on June 14, 2021).

“European Digital Infrastructure and Data Sovereignty A Policy Perspective.” Available at: https://www.eitdigital.eu/fileadmin/files/2020/publications/data-sovereignty/EIT-Digital-Data-Sovereignty-Summary-Report.pdf, (last accessed on June 14, 2021).

Federal law dated 01.05.2019 № 90-FZ "On amendments to the Federal law "On communications" and the Federal law "On information, information technologies and information protection".” *Internet Governance Project.* Available at: https://www.internetgovernance.org/wp-content/uploads/Federal-law-FZ-90-Summary.pdf, (last accessed on June 10, 2021).

FTC. “Facebook Settles FTC Charges That it Deceived Consumers by Failing to Keep Privacy Promises.” Available at: https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep, (last accessed on June 10, 2021).

FTC. (2019). “A Brief Overview of the Federal Trade Commission’s Investigative, Law Enforcement, and Rulemaking Authority.” Available at: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, (last accessed on June 14, 2021).

Fung, Brian. (2015). “AT&T will pay $25 million after call-center workers sold customer data.” *Washington Post.* Available at: https://www.washingtonpost.com/news/the-switch/wp/2015/04/08/att-will-pay-25-million-after-call-center-workers-sold-customer-data/, (last accessed on June 14, 2021).

Gaeta, Maria. “Hard Law and Soft Law on Data Protection: What A DPO should know to better perform his or her tasks.” Available at: http://www.ejplt.tatodpr.eu/Fascicolo/article_html?ida=107, (last accessed on May 29, 2021).

Gibbs, Samuel. (2017). “France orders WhatsApp to stop sharing user data without consent.” *The Guardian.* Available at: https://www.theguardian.com/technology/2017/dec/19/france-orders-whatsapp-stop-sharing-user-data-facebook-without-consent, (last accessed on June 1, 2021).

Gross, Grant. (2015). “AT&T call centers sold mobile customer information to criminals.” *Computer World.* Available at: https://www.computerworld.com/article/2907223/att-call-centers-sold-mobile-customer-information-to-criminals.html, (last accessed on June 11, 2021).

Guidelines 01/2021 on Examples Regarding Data Breach Notification. European Data Protection Board, 2021. Available at: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.

Hill, Jonah Force. (2012). "A Balkanized Internet?: The Uncertain Future of Global Internet Standards." *Georgetown Journal of International Affairs*, 2012, 49-58. Available at: http://www.jstor.org/stable/43134338, (last accessed on June 14, 2021).

Hill, Kashmir. (2014). "'God View': Uber Allegedly Stalked Users for Party-Goers' Viewing Pleasure (Updated)." *Forbes.* Available at: https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/?sh=bc90ad931411, (last accessed on June 8, 2021).

Hobbs, Carla. (2020). "Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry." *European Council on Foreign Relations.* Available at: https://ecfr.eu/wp-content/uploads/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf, (last accessed on June 14, 2021).

Hoboken, Joris and Rubinstein, Ira. (2014). "Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era." *66 ME L. Rev. 487.* Available at: https://digitalcommons.mainelaw.maine.edu/cgi/viewcontent.cgi?article=1092&context=mlr, 488, (last accessed on June 10, 2021).

Hofmann, Jeanette. (2016). "Multi-stakeholderism in Internet governance: putting a fiction into practice." *Journal of Cyber Polic*y, 1(1), 29-49, DOI: 10.1080/23738871.2016.1158303.

Hohmann, Mirko. (2014). "Technological Sovereignty: Missing the Point?" *Global Public Policy Institute.* Available at: https://www.gppi.net/2014/11/24/technological-sovereignty-missing-the-point, (last accessed on June 2, 2021).

Hong Shen. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication* 9:3, pages 304-324.

ICANN. "About." *ICANN Public Meetings.* Available at: https://meetings.icann.org/en/about, (last accessed on June 5, 2021).

Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021.

Iyengar, Rishi. (2018). "The Future of the Internet Is Indian." *CNN Business.* Available at:

https://edition.cnn.com/interactive/2018/11/business/internet-usage-india-future/, (last accessed on June 14, 2021).

Jarke, Matthias. (2020). "Data Sovereignty and the Internet of Production." *Advanced Information Systems Engineering*, 549–58. https://doi.org/10.1007/978-3-030-49435-3_34., 549, (last accessed on June 9, 2021).

John Palfrey, Clifford Chen, Sam Hwang, and Noah Eisenkraft. "Public Participation in ICANN." Available at: https://cyber.harvard.edu/icann/publicparticipation/, (last accessed on June 14, 2021).

JUSTICE K S PUTTASWAMY (RETD.), AND ANR. VS UNION OF INDIA AND ORS [2017] WRIT PETITION NO 494 OF 2012. Available at: https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

Kalra, Aditya. (2021). "India's draft e-commerce policy calls for equal treatment of sellers." *Reuters* (online). Available at: https://www.reuters.com/article/us-india-ecommerce-policy-idUSKBN2B50DT, (last accessed on June 14, 2021).

Kapur, Akash. (2019). "The Rising Threat of Digital Nationalism." *Wallstreet Journal.* Available at: https://www.wsj.com/articles/the-rising-threat-of-digital-nationalism-11572620577, (last accessed on June 13, 2021).

Kesan, Jay P. and Gallo, Andres. (2008). "Pondering the Politics of Private Procedures: The Case of ICANN" (November 6, 2007). *I/S A Journal of Law and Policy*, Vol. 4, pp. 345-409, Illinois Public Law Research Paper No. 07-11, Available at SSRN: https://ssrn.com/abstract=1028128, (last accessed on June 10, 2021).

Kittane, P., Charles, I., S., Kamath, A., Gokhale, G. (2021). "Privacy and Data Protection – India Wrap 2020." Available at: https://www.natlawreview.com/article/privacy-and-data-protection-india-wrap-2020, (last accessed on June 14, 2021).

Kovacs, A., Ranganathan, N. (2019). Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India. Data Governance Network Working Paper 03.

Kurth, Hunton., Andrews. (2021). "India Releases Revised Non-Personal Data Framework." Available at: https://www.natlawreview.com/article/india-releases-revised-non-personal-data-framework, (last accessed on June 14, 2021.)

Kwet, Michael. (2019). "Digital Colonialism: US Empire and The New Imperialism in The Global South". *Race & Class* 60 (4): 3-26. doi:10.1177/0306396818823172.

Lewis, James Andrew. "Sovereignty and the Evolution of Internet Ideology." *Center for Strategic and International Studies*. https://www.csis.org/analysis/sovereignty-and-evolution-internet-ideology, (last accessed on June 10, 2021).

Mandavia, Meghan. (2020). "Parliamentary panel invites comments on personal data protection bill." *The Economic Times.* Available at: https://economictimes.indiatimes.com/news/politics-and-nation/parliamentary-panel-invites-comments-on-personal-data-protection-bill/articleshow/73589688.cms?from=mdr, (last accessed on June 12, 2021).

Marda, Vidushi. (2020). “Non-personal data: the case of the Indian Data Protection Bil, Definitions and Assumptions.” Available at: https://www.adalovelaceinstitute.org/blog/non-personal-data-indian-data-protection-bill/, (last accessed on June 14, 2021).

Market Study on the Telecom Sector In India – Key Findings and Observations. New Delhi: Competition Commission of India, 2021. Available at: https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-Study-on-the-Telecom-Sector-In-India.pdf, (last accessed on June 10, 2021).

Martindale, Jon. (2018). “From pranks to nuclear sabotage, this is the history of malware.” *Digital Trends.* Available at: https://www.digitaltrends.com/computing/history-of-malware, (last accessed on June 14, 2021).

Mundie, Craig. (2014). "Privacy Pragmatism: Focus on Data Use, Not Data Collection." *Foreign Affairs* 93, no. 2: 28-38. Available at: http://www.jstor.org/stable/24483581, (last accessed on June 5, 2021).

Michèle Finck and Frank Pallas. (2020). “They who must not be identified—distinguishing personal from non-personal data under the GDPR.” *International Data Privacy Law*, Volume 10, Issue 1Pages 11–36, Available at: https://doi.org/10.1093/idpl/ipz026.

Mooy, Michelle De. (2017). “Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data.” Available at: https://cdt.org/wp-content/uploads/2017/04/Rethinking-Privacy_2017_final.pdf, (last accessed on June 14, 2021).

Negro, Gianluigi. (2020). “A history of Chinese global Internet governance and its relations with ITU and ICANN.” *Chinese Journal of Communication*, 13:1, 104-121, DOI: 10.1080/17544750.2019.1650789.

“Openness Key Principle of Internet Governance Says UNESCO.” (2004). http://www.unesco.org/new/en/member-states/single-view/news/openness_key_principle_of_internet_governance_says_unesco/, (last accessed on June 10, 2021).

Palfrey, John. (2004.) The end of the experiment: How ICANN's foray into global internet democracy failed. Harvard Journal of Law & Technology 17(2): 409-473.

Personal Data Protection Bill, 2019. http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf (last accessed on June 12, 2021).

Pohle, J. & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

Polatin-Reuben, Dana, and Joss Wright. (2014). "An Internet with BRICS Characteristics: Data Sovereignty And The Balkanisation Of The Internet", 1-10. Available at:

https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben, (last accessed on June 14, 2021).

Pramanik, Ayan. (2017). "Need policy against data colonisation: Nandan Nilekani." *Business Standard*. Available at: https://www.business-standard.com/article/technology/need-policy-against-data-colonisation-nandan-nilekani-117080900007_1.html, (last accessed on June 13, 2021.)

Press Trust of India. "Active internet users likely to reach 900 mn by 2025: IAMAI." *Business Standard.* Available at: https://www.business-standard.com/article/technology/active-internet-users-in-india-likely-to-reach-900-mn-by-2025-iamai-121060300710_1.html, (last accessed on June 12, 2021).

Press Trust of India. (2019). "India's data must be controlled by Indians: Mukesh Ambani." *Mint.* Available at: https://www.livemint.com/Companies/QMZDxbCufK3O2dJE4xccyI/Indias-data-must-be-controlled-by-Indians-not-by-global-co.html, (last accessed on June 14, 2021).

Press Trust of India. (2020). "India 'important digital power' won't compromise on data sovereignty: Ravi Shankar Prasad," *Economic Times.* Available at: https://economictimes.indiatimes.com/tech/ites/india-important-digital-power-wont-compromise-on-data-sovereignty-prasad/articleshow/76840586.cms, (last accessed on June 14, 2021).

Press Trust of India. (2021). "Any attempt to create 'imperialism of internet' by few companies unacceptable: Ravi Shankar Prasad," *Financial Express.*

Privacy Act of 1974. Available at: https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20of%201974,of%20records%20by%20federal%20agencies.

"Proposal for a Regulation on European data governance (Data Governance Act)." Available at: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-data-governance-data-governance-act, (last accessed on June 3, 2021).

Purpose of the Cloud Act. Available at: https://www.justice.gov/dag/page/file/1153466/download.

Ranganathan, Nayantara. 2019. "The seduction of data sovereignty in India." *Hindustan Times.* Available at: https://www.hindustantimes.com/analysis/the-seduction-of-data-sovereignty-in-india/story-iOS8cVKxstIIgJLy47Iy0J.html, (last accessed on June 9, 2021).

Report by the Committee of Experts on Non-Personal Data Governance Framework.

"Revised Report by the Committee of Experts on Non-Personal Data Governance Framework." (2021). *Trilegal.* Available at: https://www.trilegal.com/index.php/publications/analysis

/revised-report-by-the-committee-of-experts-on-non-personal-data-governance (last accessed on June 12, 2021).

Robin, Patrice. (2018). "Trend Analysis: Cyber Sovereignty and Data Sovereignty." *CSS Cyber Defense Project.* Available at: https://www.researchgate.net/profile/MarieBaezner/publication/325335882_Trend_Analysis_Cyber_Sovereignty_and_Data_Sovereignty/links/5bebbdc34585150b2bb4f0ef/Trend-Analysis-Cyber-Sovereignty-and-Data-Sovereignty.pdf, (last accessed on June 10, 2021).

"Russia's Assault on Freedom of Expression." (2017). *HRW.* Available at: https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression, (last accessed on June 7, 2021.)

"Russia: Growing Internet Isolation, Control, Censorship." (2020). *HRW.* Available at: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship#:~:text=Russian%20internet%20users.-,The%20Sovereign%20Internet%20Law,state's%20control%20over%20internet%20infrastructure, (last accessed on June 7, 2021).

Séverine Arsène. The impact of China on global Internet governance in an era of privatized control. Chinese Internet Research Conference, May 2012, Los Angeles, United States.

Sharma, Rajat. (2021). "There can be no compromise on India's digital sovereignty: Ravi Shankar Prasad." Available at: https://www.indiatvnews.com/news/india/there-can-be-no-compromise-on-india-s-digital-sovereignty-ravi-shankar-prasad-aaj-ki-baat-rajat-sharma-opinion-blog-707857, (last accessed on June 10, 2021).

Singh, Shiv Shankar. "Privacy and Data Protection in India: A Critical Assessment." *Journal of the Indian Law Institute* 53, no. 4 (2011): 663-77. http://www.jstor.org/stable/45148583, (last accessed on June 8, 2021).

Sleinan, Julett. (2021). "Experts Concerned About Growing Censorship in Russia." *Organized Crime and Corruption Reporting Project.* Available at: https://www.occrp.org/en/daily/14074-experts-concerned-about-growing-censorship-in-russia, (last accessed on May 24, 2021).

Snipp, C Matthew. (2016). "What Does Data Sovereignty Imply: What Does It Look Like?" In *Indigenous Data Sovereignty: Toward an Agenda*, edited by KUKUTAI TAHU and TAYLOR JOHN, 39-56. Acton ACT, Australia: ANU Press. Available at: http://www.jstor.org/stable/j.ctt1q1crgf.10, (last accessed on June 9, 2021).

Stifel, Megan. (2017). "Maintaining U.S. Leadership on Internet Governance." Available at: https://www.cfr.org/report/maintaining-us-leadership-internet-governance, (last accessed on June 11, 2021).

SWAMI *RAMDEV & ANR. versus FACEBOOK, INC.. & ORS [2019]*. Available at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/01/Ramdev-v.-Facebook-Delhi-HC.pd (last accessed on June 10, 2021).

Telecom Regulatory Authority of India. "The Indian Telecom Services Performances Indicator April – June 2020." TRAI: New Delhi, India. Available at: https://trai.gov.in/sites/default/files/Report_09112020_0.pdf (last accessed on June 10, 2021).

"The Digital Services Act: Ensuring a safe and accountable online environment." Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en#new-rules-in-a-nutshell, (last accessed on June 3, 2021).

"The Digital Services Act package." Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package, (last accessed on June 3, 2021).

"The Extra-Territorial Reach of EU Data Protection Law." (2019). Available at: https://www.sidley.com/en/insights/publications/2019/07/the-extra-territorial-reach-of-eu-data-protection-law, (last accessed on May 29, 2021).

Tripathi, Karan. (2020). "'Why Are you Aggrieved By Global Injunction Order?': Delhi HC Asks Facebook In Baba Ramdev's Case." *LiveLaw.in*. (last accessed on June 2, 2021).

Ünver, Akin. (2018). "Politics of Digital Surveillance, National Security and Privacy." Available at: https://edam.org.tr/wp-content/uploads/2018/04/Chrest_Surveillance2.pdf, (last accessed on June 14, 2021).

U.S. Department of Health & Human Services. "Summary of the HIPAA Security Rule." Available at: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

"US: Police Found to Violate Fellow Officer's Privacy: Minnesota Case Shows Need for Stronger Data Protection Laws." (2019). *Human Rights Watch.* Available at: https://www.hrw.org/news/2019/06/20/us-police-found-violate-fellow-officers-privacy, (last accessed on June 10, 2021).

Van Klyton, Aaron and Soomaree, Ayush and Arrieta-Paredes, Mary-Paz, The Multistakeholder Model of Internet Governance, ICANN, and Business Stakeholders - Practices of Hegemonic Power (January 22, 2018). GigaNet: Global Internet Governance Academic Network, Annual Symposium 2017, Available at SSRN: https://ssrn.com/abstract=3107291, (last accessed on June 8, 2021).

Veni Markovski and Alexey Trepykhalin, Country Focus Report: Russian Federation Internet-Related Laws and United Nations Deliberations, ICANN (2021), pg.3, available at: https://www.icann.org/en/system/files/files/ge-006-19jan21-en.pdf, (last accessed on June 14, 2021).

Weinberg, Jonathan. (2011). *Governments, Privatization, and Privatization: ICANN and the GAC*, 18 Mich. Telecomm. & Tech. L. Rev. 189.

Weinberg, Jonathan. (2000). "ICANN and the Problem of Legitimacy." *Duke Law Journal* 50, no. 1: 187-260. (last accessed on June 2, 2021). doi:10.2307/1373114.

Williams, Betsy Anne, Catherine F. Brooks, and Yotam Shmargad. (2018). "How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications." *Journal of Information Policy* 8 78-115, (last accessed on June 14, 2021). doi:10.5325/jinfopoli.8.2018.0078.

Wilson, E. J. (2005). "What is Internet Governance and Where Does it Come From?" Journal of Public Policy 25: 29 – 50.

Wimmer Kurt, CIPP/E, CIPP/US, Maldoff, Gabe, and Lee, Diana. (2020). "Comparison: Indian Personal Data Protection Bill 2019 vs. GDPR." *Iapp.* Available at: https://iapp.org/media/pdf/resource_center/india_pdpb2019_vs_gdpr_iapp_chart.pdf.

Winter, Jenifer Sunrise. (2018). "Introduction to the Special Issue: Digital Inequalities and Discrimination in the Big Data Era." *Journal of Information Policy* 8: 1-4. doi:10.5325/jinfopoli.8.2018.0001.

Woods, Andrew. (2018). "Litigating Data Sovereignty". Yale Law Journal, 328 - 406.

Wulf, W. A., & Jones, A. K. (2009). Reflections on Cybersecurity. *Science*, 326, no. 5955, 943-944.

"5 Examples of Data & Information Misuse." *ObserveIt*. Available at: https://www.observeit.com/blog/importance-data-misuse-prevention-and-detection/, (last accessed on June 7, 2021).

About ICRIER

Established in August 1981, ICRIER is a policy-oriented, not-for-profit, economic policy think tank. ICRIER's main focus is to enhance the knowledge content of policy making by undertaking analytical research that is targeted at informing India's policy makers and also at improving the interface with the global economy.

ICRIER has two office locations in Delhi; in the institutional complex of India Habitat Centre and a new office at the Institutional Area, Sector 6, Pushp Vihar, New Delhi.

ICRIER's Board of Governors include leading academicians, policymakers, and representatives from the private sector. Mr. Pramod Bhasin is ICRIER's chairperson and Dr. Deepak Mishra is Director & Chief Executive.

ICRIER conducts thematic research in the following five thrust areas:

1. Growth, Employment and Macroeconomics (GEM)
2. Trade, Investment and External Relations (TIER)
3. Agriculture Policy, Sustainability and Innovation (APSI)
4. Digital Economy, Start-ups and Innovation (DESI)
5. Climate Change, Urbanization and Sustainability (CCUS)

To effectively disseminate research findings, ICRIER organises workshops, seminars and conferences to bring together academicians, policymakers, representatives from industry and media to create a more informed understanding on issues of major policy interest. ICRIER routinely invites distinguished scholars and policymakers from around the world to deliver public lectures and give seminars on economic themes of interest to contemporary India.