“THE CLOUDS OF A BLOODLESS WAR”: DATA LOCALISATION AND THE SECURITISATION OF CYBERSPACE IN INDIA

By

Konstantin Urban

Submitted to
Central European University
Department of International Relations

In partial fulfillment of the requirements for the degree of Masters, International Relations

Supervisor: Xymena Kurowska

Vienna, Austria
2021

Abstract

Data localisation has been the latest buzzword within national cybersecurity discourses. Governments across the spectrum have advocated for localizing data for numerous reasons from circumventing foreign surveillance to alleviating data access to local law enforcement agencies to protecting its citizen's privacy. Yet, apart from not quite fulfilling its stated objectives, localizing data can actually facilitate the government's surveillance and censorship efforts. Indeed, while the common denominator for advocating data localisation is security, such efforts tend to make the data less secure. This is the paradox this thesis explores. Through the use of Copenhagen School's securitisation theory and the concept of technification as developed by Hansen and Nissenbaum, this thesis questions the role of data localisation in the securitisation of cyberspace. Taking the data localisation discourse in India, with a special focus on the country's "digital strike" that banned a number of Chinese mobile apps, as the case study, the thesis argues that data localisation is itself a securitising move that securitizes cyberspace through technification.

Acknowledgements

I would like to give my special gratitude to my supervisor, Professor Xymena Kurowska for their continuous support and guidance, constructive criticism, and encouraging feedbacks.

I would also like to thank my brother for regularly checking in how I was doing during this stressful time.

Finally, not to mention, my wonderful friends Richard and Gustav who have kept me motivated through their shenanigans, words of encouragement and great conversations.

Table of Contents

Introduction

At the inauguration of the Digital India[1] week, the current Prime Minister Narendra Modi proclaimed he “dream[s] of [a] Digital India where cyber security becomes [an] integral part of national security” and in alluding to the dangers looming in cyberspace noted that “clouds of a bloodless war are hovering” over the world and that “India has a big role to play in this.”[2] Modi’s statement reflects sentiments of the enormous potential and risks that the digital revolution and by extension cyberspace presents for India. On the one hand, India has a burgeoning IT sector that is expected to grow 14-fold by 2030, from US$35bn in 2019.[3] On the other hand, however, the country’s increasing reliance on cybertechnologies for government services and exponential growth in internet users, projected to amount to close to a billion in the next four years[4], presents the government with major challenges from disinformation, to cybercrime to cyberterrorism to foreign surveillance. As such, cybersecurity has become an ever-salient issue within the country’s national security discourse.

One aspect where India has been particularly vocal is in matters pertaining to data, specifically in terms of its ownership, storage, and processing. To better understand India’s position pertaining to its drive to localise data, however, it is important to note that since 2014 the country has been ruled by the Bharatiya Janata Party (BJP).[5] The BJP itself is an

[1] “Digital India is a flagship programme of the Government of India with a vision to transform India into a digitally empowered society and knowledge economy.” https://www.digitalindia.gov.in/

[2] World Facing 'Bloodless' Cyber War Threat: Modi,” The Hindu (The Hindu, April 1, 2016), https://www.thehindu.com/news/national/world-facing-bloodless-cyber-war-threat-modi/article7375190.ece.

[3] Hinrich Foundation and All India Management Association, (2019), *The Data Opportunity: The Promise of Digital Trade for India.* https://alphabeta.com/wp-content/uploads/2019/08/digitrade_india.pdf

[4] “Number of internet users in India from 2015 to 2020 with a forecast until 2025.” https://www.statista.com/statistics/255146/number-of-internet-users-in-india/

[5] Safi, Michael. “India Election Results 2019: Modi Claims Landslide Victory,” The Guardian (Guardian News and Media, May 23, 2019), https://www.theguardian.com/world/2019/may/23/india-election-results-narendra-modi-bjp-victory.

offshoot of the Rashtriya Swayamsevak Sangh (RSS), a right-wing, Hindu nationalist, paramilitary volunteer organisation.[6] Indeed, sentiments reflecting the need for data localisation are reflected in statements by prominent BJP politicians from the current administration who, for instance, assert "they [the West as a 'colonial' entity] had come for spices, now they [the West as a 'neo-colonial' entity] would come for data. They ruled us after taking the spice, now they will rule us after taking the data."[7] As will be explored there is an understanding that India's sovereignty is incomplete if it is not able to govern over the data that is generated and flows through its borders and hence also presents a major national security threat. Data localisation, as it is commonly termed, has been argued for through a number of justifications from it being a critical national resource that would propel the Indian economy to ensuring that Indian data remains safe and secure.

Yet, apart from not quite fulfilling its stated objectives, localizing data can actually facilitate the government's surveillance and censorship efforts. As such, the central research question this thesis seeks to explore is: *what is the role of data localisation in the securitisation of the cyberspace?* The argument is that data localisation itself is a securitising move and hence questions whether security can be separated from the conversation on data localisation. It is, after all, an intriguing paradox, while the common denominator for advocating data localisation is security, such efforts make the data less secure. As such, the thesis will elucidate how the physical, the purely technical aspects of cyberspace have become an avenue to pursue social, political, and economic agendas in the name of security. Ultimately, the thesis aims to fill a certain gap in the literature, one that understands data localisation as a move that securitizes cyberspace through technification.

[6] D.K. Singh, "Between Vajpayee and Modi Era, RSS Has Learnt Many Political Lessons," ThePrint, February 22, 2021, https://theprint.in/opinion/politically-correct/between-vajpayee-and-modi-era-rss-has-learnt-many-political-lessons/609419/.

[7] Sahgal, Priya. "Decoding Data Sovereignty: The Pursuit of Supremacy, Cover Story Special," YouTube (NewsX, June 10, 2019), https://www.youtube.com/watch?v=RVB8UapHvdQ&t=300s

The distinctive technical specificities of cybertechnology coupled with its widespread social and national engagement has created an antagonistic zero-sum environment that allows for a plethora of real but also deliberately constructed security threats. Security, after all, is not objective.[8] Security, when it pertains to cyberspace is often framed in two parallel ways: one that is focused purely on the technical functionalities and security of the individual, and another constructed through socio-political processes that are linked to traditional ideas of national security.[9] This, however, is problematic because technology is "political to its very core"[10] and threats to the security of a nation often warrant extraordinary measures that tend to limit the civil liberties of its citizens, hence the necessity to scrutinize why a certain state of security is needed and if corresponding regulations are justified.[11] This is where the Copenhagen School's theory of securitisation with its understanding of "security as a discursive modality"[12] is particularly useful because it helps one explain how and why issues are constructed as security concerns and the effects this process can have on communities.[13]

Hansen and Nissenbaum have expanded the securitisation framework to include cybersecurity and have identified three security modalities.[14] Albeit overlapping, the focus of this thesis will be "technification."[15] The fact that computer security is a complex subject knowable only to a specific group of people i.e. computer and information scientists, who are well versed in the technicalities of this field, they are permitted heightened legitimacy to formulate issues in cybersecurity.[16] This group is then able to transcend the role of traditional

[8] Buzan, Barry, Ole Wæver and Jaap De Wilde. *Security: A new framework for analysis*. Lynne Rienner Publishers, 1998.

[9] Nissenbaum, Helen. "Where Computer Security Meets National Security." In *Cybercrime*, pp. 59-84. New York University Press, 2007.

[10] Ibid, p. 62.

[11] Ibid, p. 70.

[12] Ibid, p. 1155.

[13] Buzan, Barry, Ole Wæver and Jaap De Wilde. *Security: A new framework for analysis*. Lynne Rienner Publishers, 1998.

[14] Hansen, Lene, and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." *International studies quarterly* 53, no. 4 (2009): 1155-1175, p. 1157.

[15] Ibid, p. 1157.

[16] Ibid, p. 1167.

security experts and speak directly to the larger public in a manner that both facilitates and supports the cyber-related threats propagated by politicians and the media.[17]

By taking India as a case study to further the discussion, the thesis seeks to explore the role of data localisation in India's national cybersecurity discourse. How is the argument framed and under what pretexts? Who are the securitising actresses calling for data localisation and how are localising measures correspond to their stated objectives? Indeed, following the border conflict at the Line of Actual Control (LAC) in the Galwan Valley in the summer of 2020, the Government of India (GoI) responded with a "digital strike"[18] that has since banned over 200 Chinese apps and prohibited the use of Huawei and ZTE products in the construction of the country's 5G infrastructure.[19] How do these policies play into India's data localisation rhetoric and broader securitisation of cyberspace?

As such, this thesis is structured into three chapters. The first chapter, "Technification as a securitizing move" lays out the theoretical framework based on the Copenhagen School's securitisation theory while focusing on the concept of technification. The second chapter, "Data localisation as a security discourse" provides a literature review and maps out India's data localisation discourse within it. The final section, "India's 'digital strike'" provides a holistic elucidation of the argument by appraising the country's unanimous banning of a number of Chinese apps.

Chapter 1: Technification as a securitising move

[17] Ibid.

[18] "India's Digital Strike on China: After Chinese Apps' Ban, Govt Trains Guns on Fintech Firms," Business Today, September 22, 2020, https://www.businesstoday.in/current/corporate/indias-digital-strike-on-china-chinese-apps-ban-fintech-firms-on-govts-radar-mobile-based-lenders/story/416687.html.

[19] "India's Decision to Allow 5G Trials without Huawei, ZTE a Sovereign Step: US," Business Today, May 12, 2021, https://www.businesstoday.in/current/economy-politics/india-decision-to-allow-5g-trials-without-huawei-zte-a-sovereign-step-us/story/438830.html.

The primary theoretical framework used in this project is Copenhagen School's theory of securitisation. This theory is particularly useful because of its understanding of security as something that has to be meticulously constructed through discourse. It is within this concept that we will appraise how the cyber realm is understood to be threatening, as such designated as a security issue and warranting particular policy measures. Specifically, this thesis uses Hansen's and Nissenbaum's concept of "technification" and asserts that the shrouding of cyber matters in technical terms comprehendible only to some, and the placement of technical experts within decision-making positions, is a securitising move in and of itself.

1.1 Securitisation Theory

In the most basic terms, the theory of securitisation traces how issues in society become issues in the first place. George W. Bush was successful in convincing the American public that Saddam Hussein had stockpiles of weapons that were threatening their security and as such was able to go to war with Iraq.[20] Several European governments have been able to persuade their populous that an influx of migrants would negatively affect their social wellbeing and have employed restrictive immigration policies.[21] In India, the Hindutva has been propagating "love jihad" which accuses Muslim men of forcibly converting Hindu women by marriage leading to restrictions in interfaith marriage in some states.[22] It suffices to say that often security issues do not necessarily reflect their objective and material circumstances but on the contrary are specifically designed by key actresses to garner some

[20] Vultee, Fred. "Securitization: A new approach to the framing of the "war on terror"." *Journalism practice* 4, no. 1 (2010): 33-47.

[21] Léonard, Sarah. "EU border security and migration into the European Union: FRONTEX and securitisation through practices." *European security* 19, no. 2 (2010): 231-254.

[22] Gupta, Charu. "Hindu women, Muslim men: Love Jihad and conversions." *Economic and Political Weekly* (2009): 13-15.

desired outcome.[23] As such the primary goal of securitisation theory is to understand how and why this happens and what the potential outcomes of this are on the social, political, and economic processes of communities.[24] In the words of its authors, Barry Buzan, Ole Wæver, and Jaap De Wilde, "securitization studies aims to gain an increasingly precise understanding of who securitizes, on what issues (threats), for whom (referent objects), why, with what results and, not least, under what conditions (what explains when securitization is successful)."[25]

So, what is securitisation theory? The most commonly used definition notes that "when a securitizing actor uses a rhetoric of existential threat and thereby takes an issue out of what under those conditions is "normal politics,"[26] we have a case of securitization."[27] As such, "securitisation is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects."[28] In other words, the theory asserts that security and threats are not objective but rather crafted by a securitising actress through a "speech act" as extraordinarily threatening and imminent, thus warranting extreme measures. The success of a securitising act, however, is dependent on its acceptance by a relevant audience.

Another way of understanding securitisation is to see it as an exaggerated form of politicisation.[29] If an issue is not politicized "the state does not deal with it, and it is not in any other way made an issue of public debate and decision."[30] If an issue is politicised "the issue is part of public policy, requiring government decision and resource allocations or,

[23] Buzan, Barry, Ole Wæver, and Jaap De Wilde. *Security: A new framework for analysis*. Lynne Rienner Publishers, 1998.
[24] Ibid.
[25] Ibid, p. 32.
[26] Not all scholars subscribe to the dichotomy of "normal" and "exceptional" politics. See for instance: Salter, Mark, and Thierry Balzacq. "Securitization Theory: How security problems emerge and dissolve." (2011).
[27] Buzan, Barry, Ole Wæver, and Jaap De Wilde. *Security: A new framework for analysis*. Lynne Rienner Publishers, 1998, p. 24-25.
[28] Ibid.
[29] Ibid, p. 23.
[30] Ibid.

more rarely, some other form of communal governance."[31] If, however, an issue is securitised, the issue gains a status of being "special" or "above politics" and dealt with in an accelerated manner by foregoing conventional rules and political processes.[32] Within democratic regimes wherein public debates are an integral aspect, these distinctions are important to note because a nonpoliticized issue does not mean it is unimportant only because it is not talked about. On the contrary, it means an issue and corresponding policy recommendations do not undergo the same level of scrutiny and deliberation, which can consequently result in policies that adversely affect society. Since security issues regarding the cyber realm have not yet reached the saliency of, for instance, environmental issues, and since the nitty-gritties of cybersecurity are only understandable to a select few, policy regulations in this field are rarely politicised but often securitized.

For an issue to be securitized it is reliant upon a certain speech act.[33] Borrowing from the speech act literature, the premise suggests that, beyond simply expressing information regarding an issue, language also has a performative character that influences and transforms social reality.[34] Through the use of certain words, like 'security' for instance, one can influence thought processes because beyond the literal definition of words, their connotative meanings can have denotative effects. This is then complemented by linguistic tools that can increase the performative power of what is being spoken. In this sense, it is the "articulation of security" as existential and eminent that leads to "security action" thereby structuring the potential "social practices that follow."[35] One aspect that this emphasis on linguistic utterance often overlooks, however, is how the discourse is facilitated by actions of actresses that might

[31] Ibid.
[32] Ibid.
[33] Balzacq, Thierry, Sarah Léonard, and Jan Ruzicka. "'Securitization'revisited: Theory and cases." *International Relations* 30, no. 4 (2016): 494-531, p. 506 – 507.
[34] Ibid.
[35] Strizel, H. (2007). Towards a Theory of Securitization: Copenhagen and Beyond. European Journal of International Relations 13(3): 357–383, p. 360.

not be as vocal or visible. As such, while this “explicit verbal speech act methodology”[36] used to be the primary basis of securitisation theory, it has moved towards including explorations into regimes of practice as securitising moves that complement or even transcend the focus on rhetoric.[37] Such approaches tend to be categorised as the Paris School. Didier Bigo, for instance, holds that securitisation “comes also from a range of administrative practices” and “a specific habitus of the ‘security professional’ with its ethos of secrecy and concern for the management of fear or unease.”[38] Indeed, the capacity of state and non-state, and, private and public actresses such as experts, consultants, and bureaucrats to establish a narrative and pre-structure the discursive field have already been studied.[39] Due to the limitations of this paper, however, our analysis of data localisation and corresponding securitisation of cyberspace in India will not include Paris’s school practice-oriented approach.

Following the initial securitising move, a few more terms need elaboration to garner a complete grasp of the securitisation process. First is the securitising actress, which can be understood as the entity that engages in the security speech act by declaring something i.e. a referent object, as existentially threatened.[40] Generally, these tend to be political leaders, bureaucrats, governments, lobbyists, and pressure groups but can essentially be any entity that is able to raise enough saliency to an issue.[41] Second, the referent object can be understood as that to which one can point and say “this needs to survive and hence one must do X”, in other words it is the thing that is threatened and in need of ‘protection’.[42] While

[36] Buzan, Barry, and Lene Hansen. *The evolution of international security studies*. Cambridge University Press, 2009, p. 216.
[37] Bigo, Didier. *"Security and immigration: Toward a critique of the governmentality of unease."* Alternatives 27, no. 1_suppl (2002): 63-92.
[38] Ibid, p. 66-67.
[39] Huysmans, Jef. *The politics of insecurity: Fear, migration and asylum in the EU*. Routledge, 2006.
[40] Buzan, Barry, Ole Wæver, and Jaap De Wilde. *Security: A new framework for analysis*. Lynne Rienner Publishers, 1998, p. 36.
[41] Ibid.
[42] Ibid.

traditionally the referent objects have been the state and the nation, securitisation theory allows for a much wider spectrum of possibilities.[43] Consequently, securitising actresses can in principle declare anything as a referent object but in practice, they are reliant upon an audience that accepts it as such too.[44] Finally, functional actresses are those that can significantly influence trajectories in the field of security.[45] For example, in the environmental sector, a polluting firm can be understood as a functional actress.[46] Similarly, functional actresses in the cyber realm include private corporations like Facebook and Google. They are neither referent objects, meaning they are not threatened, nor attempt to securitise cyberspace but still hold a significant amount of power in defining regulations and modes of conduct in this space. Precisely how the cyber realm fits within the theory of securitisation will be discussed in the next section.

1.2 Securitisation Theory and Cyberspace

Although tough to imagine today, in the late 1990s, while the insecurities of cyberspace were gaining popularity, cybersecurity had not reached the radar of Security Studies because it did not quite have the "cascading effects on other security issues".[47] Cyberspace has however come a long way since then as the rise of internet connectivity around the world and devices connected to it from the smartphone to national critical infrastructure along with the numerous cyber threats to them indicate. Consequently, in one of the most cited articles in this field, Hansen and Nissenbaum, by adopting the concept of

[43] Ibid.
[44] Ibid.
[45] Ibid.
[46] Ibid.
[47] Ibid, p. 25.

securitisation as its starting point, convincingly argue for cyberspace to be included as a specific sector within the broader terrain of Security Studies.[48]

A sector can be understood as a lens or discourse that is formed through a particular collection of threats, referent objects, and grammars of securitisation.[49] Sectors, however, are not constant, but change as the reality of the world changes, such as the proliferation of cybertechnologies and the unique set of dangers they present. Indeed, threats that emerge from cyberspace are not too different from that of the economic, health, and environmental sectors. Their common denominator is the global nature of their threats, one that exceeds traditional conceptions of national-military security and thereby redefines ideas of authority and sovereignty.[50] Cyberspace is nonetheless distinct due to the "complex constellation of public-private responsibility and governmental authority."[51] After all, in the field of cybersecurity, governments tend to rely on the expertise from the private sector and also hold them co-responsible.[52] Additionally, the raw physical infrastructure that hosts this virtual space is primarily built and operated by the private sector.[53] For the most part, this has been a rather symbiotic relationship, wherein the political and economic were kept in the fine balance, however, with the growing salience of cyber-related threats to both the nation and the state, governments are in an increasingly precarious position to fulfill their role as the sole providers of national security. Furthermore, cyberspace complicates the theory of securitisation ontologically because it can simultaneously be a level of analysis and a sector meaning that securitisation happens on different levels i.e. local, regional, non-

[48] Hansen, Lene, and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." *International studies quarterly* 53, no. 4 (2009): 1155-1175, p. 1157.
[49] Ibid.
[50] Ibid.
[51] Ibid, p. 1162.
[52] Ibid.
[53] Ibid.

regional/subsystemic, and global, and across sectors i.e. environmental, political, economic, and societal.[54]

As such, Hansen and Nissenbaum note, the "political importance [of referent objects related to the cyber realm] arises from connections to the collective referent objects of 'the state,' 'society,' 'the nation,' and 'the economy.'"[55] These referent objects, they assert, are formulated as being threatened through three forms of securitisation:

> hypersecuritization, which identifies large-scale instantaneous cascading disaster scenarios; everyday security practices, that draws upon and securitizes the lived experiences a citizenry may have; and technifications, that captures the constitution of an issue as reliant upon expert, technical knowledge for its resolution and hence as politically neutral or unquestionably normatively desirable.[56]

In other words, hypersecuritisation can be thought of as compounded cyber disaster scenarios the likes of which one sees in movies like A Good Day to Die Hard[57] and the Terminator[58], the latter being more a case of threats arising from inherent vulnerabilities of computer systems, ones that are seemingly beyond human control. The strong focus on the hypothetical, considering that there are no past events through which to conjure images of such disasters, is important to note and affects the other securitisation modalities too. Everyday security practices are used by securitising actresses on two fronts. First, to convince people that they too play an important role in protecting network security, and second, to bring such images of cyber catastrophes closer to people's lived experiences "by linking elements of the disaster scenario to experiences familiar from everyday life."[59] The final form of securitisation, technification, is of particular interest for this project and will be explored in

[54] Kremer, Jan-Frederik, and Benedikt Müller, eds. *Cyberspace and international relations: Theory, prospects and challenges*. Springer Science & Business Media, 2013, 66.
[55] Hansen, Lene, and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." *International studies quarterly* 53, no. 4 (2009): 1155-1175, p. 1155.
[56] Ibid, p. 1157.
[57] Live Free or Die Hard (2007) - Theatrical Trailer [HD]. https://www.youtube.com/watch?v=8Jz-8UcCiws&t=48s
[58] The Terminator (1984) Official Trailer. https://www.youtube.com/watch?v=k64P4l2Wmeg
[59] Hansen, Lene, and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." *International studies quarterly* 53, no. 4 (2009): 1155-1175, p. 1165.

the next section. Ultimately, these securitisations work in interlocking ways and often complement each other on all levels and sectors.

1.3 Technification

As previously noted, the final security modality identified by Hansen and Nissenbaum is technification. The authors note:

> Technifications are, as securitizations, speech acts that ‘‘do something’’ rather than merely describe, and they construct an issue as reliant upon technical, expert knowledge, but they also simultaneously presuppose a politically and normatively neutral agenda that technology serves.[60]

In other words, technification is the construction of an issue as being particularly complex and shrouding it in technical jargon, ultimately allotting the issue with a flair of political impartiality. The effects of this are two-fold.

Firstly, technification limits comprehension and articulation of an issue to a select few who possess the required know-how in that subject.[61] In the cyber domain, for instance, this means allocating computer and information scientists with a privileged position within the cybersecurity discourse.[62] Since these are "not only experts, but *technical* ones", the domain of cybersecurity is technified by categorising issues in this field as part of their domain.[63] Indeed, this constructs the technical as an area that requires expert knowledge, knowledge that most politicians and the wider public do not have, hence allowing these "experts" to become securitizing actresses without being subject to the scrutiny and media attention of politicians.[64] Furthermore, as "experts", anything they do or say is accorded with a higher degree

[60] Ibid, p. 1167.
[61] Ibid.
[62] Ibid.
[63] Ibid.
[64] Ibid.

of epistemic authority and political legitimacy.[65] Technification, is as such, closely linked to Huysmans concept of "security experts."[66] These are "professionals who gain their legitimacy of and power over defining policy problems from trained skills and knowledge and from continuously using these in their work," and consequently have the power to modulate social and political practices in both the public and private domain.[67]

Secondly, technification, much like the speech act in securitisation, does not simply describe but also "do[es] something."[68] Technification earmarks issues as being reliant on technical, expert knowledge and presupposes political impartiality. Since technology is understood to be neutral, by extension is the knowledge produced by the experts of said technologies. Technocrats, as a result, are entrusted to frame cybersecurity issues in a manner that is objective and apolitical. Herein, however, is the problem because as Judith Butler notes, framing "does not simply exhibit reality" but "selectively produce[s] and enforce[s] what will count as reality."[69] In other words, the reality of issues pertaining to cyberspace becomes contingent upon a select few who understand its technical dimensions and allocates them the power of the narrative, a power can that can be manipulated by states to fit their political agendas. As such securitisation and technification should not be understood in isolation but rather in the interlocking ways that help "securitizing actors who seek to depoliticize their discourses'… through linkages to ''neutral'' technologies."[70] After all,

[65] Ibid.

[66] Huysmans, Jef. *The politics of insecurity: Fear, migration and asylum in the EU*. Routledge, 2006, p. 9.

[67] Ibid.

[68] Ibid, p. 1167.

[69] Butler, Judith. 2009. *Frames of War: When Is Life Grievable?* London: Verso, 2009. xiii.

[70] Hansen, Lene, and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." *International studies quarterly* 53, no. 4 (2009): 1155-1175, p. 1168.

technification limits the number of participants and hence narrows the space for debate thereby lowering the scrutinising threshold of the securitised issue.

While technification can be applied to a range of issues, cybersecurity is particularly susceptible to a discourse that is reliant on expert and technical knowledge.[71] First, is the rather strong emphasis on hypotheticals.[72] Second, is the formidable task of achieving mastery in this field.[73] And finally, is the pace of technological innovations and corresponding risks they present. The combination of these characteristics of cybersecurity further legitimises the few people who know the subject matter and hence can speak confidently towards hypotheticals[74]. These are complemented by the fact that the field is also shrouded in business and military secrecy. Indeed, while the average follower can gain a preliminary grasp of what is going on, Nissenbaum notes ‘‘that much is withheld or simply not known, and estimates of damage strategically either wildly exaggerated or understated.’’[75] Such secrecy often facilitates the formulation of “radical threats with techno-utopian solutions” that sidestep “the systemic, inherent ontological insecurity” of computer systems and “invokes an inherent tension between disaster and utopia as the future of cybersecurity.”[76]

Concludingly, securitisation in cyberspace is maintained through the process of technification wherein cybersecurity is deemed “so critical it should not be left to amateurs,” hence privileging the role and knowledge produced by technical experts.[77]

[71] Ibid.
[72] Ibid.
[73] Ibid.
[74] Ibid.
[75] Nissenbaum, Helen. "Where Computer Security Meets National Security." In *Cybercrime*, pp. 59-84. New York University Press, 2007, p. 72.
[76] Hansen, Lene, and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." *International studies quarterly* 53, no. 4 (2009): 1155-1175, p. 1167.
[77] Ibid.

When it comes to data, and consequently data localisation, one first has to ask, how often does the average internet user think about data when interacting with it? It is safe to say, for a large majority the answer would be 'extremely rare' to 'never'. The booming industry of surveillance capitalism[78] and a culture of 'I consent'[79] certainly reflects this. Partly this has to do with people simply not caring enough, after all, one can agree, for the most part, everyday experiences on cyberspace for most people is 'safe.' But, the flip side of this, is the lack of understanding of the role that data plays in all matters of the Internet because it is extremely complex, multidimensional and technical. This sets up data localisation as an ideal field to be technified in an effort to securitise the broader cyberspace.

Chapter 2: Data localisation as a security discourse

Data localisation is at first glance a purely technical matter i.e. controlling the flow of data over a network, yet much like the broader governance of internet infrastructure, it has become an avenue to pursue political agendas. Data localisation has been argued for by governments across the spectrum to circumvent foreign surveillance, promote the security and privacy of its citizens, alleviate data access to local law enforcement agencies and regulate content, stimulate domestic investment and innovation and garner a degree of data sovereignty.[80] Yet apart from the fact that data localisation goes against the fundamental principles of the internet itself, as will be explored in this section, these data localisation measures often do not achieve their stated goals. In fact, localising data potentially makes

[78] Zuboff, Shoshana. "Big other: surveillance capitalism and the prospects of an information civilization." *Journal of Information Technology* 30, no. 1 (2015): 75-89.
[79] McStay, Andrew. "I consent: An analysis of the Cookie Directive and its implications for UK behavioral advertising." *New Media & Society* 15, no. 4 (2013): 596-611.
[80] Chander, Anupam, and Uyên P. Lê. "Data nationalism." *Emory Law Journal* 64 (2014): 677 – 739.

data less secure, can increase possibilities for surveillance, and possibly harms innovation and the domestic economy. It is indeed an intriguing paradox, while the common denominator for advocating data localisation is security, such efforts actually make the data less secure. Following a literature review encompassing these topics and placing them in the context of India, this section concludes by highlighting a certain gap in the literature, one that understands data localisation not as an effort to make data more secure or protect user's privacy, but as a move that securitizes cyberspace through technification.

2.1 Data-localisation: the what

On the technical front, data localisation has broadly two meanings.[81] One is a policy wherein national governments require that data generated within national boundaries be physically stored within them.[82] This data can be their sole copies kept within local jurisdictions or mirrors that are allowed to cross borders for storage and or processing. Another meaning of data localisation is known as "localised data routing."[83] These are provisions that require internet service providers to route data packets between users in one country through infrastructures located within that jurisdiction.[84] This thesis addresses primarily the first type since that is the primary direction of India's data localisation measures.

On the social front, data localisation is a measure that goes against the fundamental principles of the technology it is built on, i.e. the Internet. The Internet was developed as a decentralised form of communication wherein every end-user could freely communicate with

[81] Basu, Arindrajit et. al., *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India* (Pranav M Bidrae et. al. eds., The Centre for Internet Society, Mar. 19, 2019), p. 11.
[82] Ibid.
[83] Ibid.
[84] Ibid.

each other.[85] It was designed to be an open space wherein authority was shared among its users, a "digital utopia" of sorts where traditional forms of governance would be rendered irrelevant.[86] Yet, the internet has come a long way since the publishing of John Perry Barlow's manifesto, "A Declaration of the Independence of Cyberspace", in 1996.[87] It certainly isn't quite the independent space envisioned by its founders. Data localisation reflects the shifting understanding of what the Internet is, from "a borderless, well-functioning, economically efficient communications network" to "a quagmire of special interests, competing political agendas and international bureaucracy."[88]

2.2 Data-localisation: the whys and their sophistries

2.2.1 Data sovereignty

Measures pertaining to the localisation of data can at first hand be understood as an attempt by governments to gain a manner of independence, control, and autonomy over a space and technology that fundamentally contradicts the idea of national sovereignty and is as such closely linked to ideas of digital and cyber sovereignty.[89] As Pohle and Thiel note, digital sovereignty "seeks to reinstate the nation state, including the national economy and the nation's citizens, as a relevant category in the global governance of digital infrastructures and the development of digital technologies."[90] The concept of sovereignty, as it applies to

[85] Komaitis, Konstantinos. "The 'wicked problem'of data localisation." *Journal of Cyber Policy* 2, no. 3 (2017): 355-365, p. 358.
[86] Ibid, p. 357.
[87] Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." *Electronic Frontier Foundation*. https://www.eff.org/cyberspace-independence.
[88] Foroohar, Rana. "The Internet Splits Up," Newsweek, March 13, 2010, https://www.newsweek.com/internet-splits-110491.
[89] Couture, Stephane, and Sophie Toupin. "What does the notion of "sovereignty" mean when referring to the digital?." *new media & society* 21, no. 10 (2019): 2305-2322.
[90] Pohle, Julia, and Thorsten Thiel. "Digital sovereignty." *Internet Policy Review* 9, no. 4 (2020), p. 2.

the digital sphere, however, is elusive because it has been conceptualized differently by different types of actresses, therefore it becomes important to ask "who defines technological sovereignty and related concepts [such as digital or cyber or data sovereignty] and for which purposes?."[91] After all, as noted by Laura DeNardis in her scholarship on Internet governance, "arrangements of technical architecture are also arrangements of power."[92] In other words, measures such as data localisation, while seemingly purely technical, have far wider consequences than the technology itself. As such, data sovereignty, in the words of Polatin-Reuben and Wright is "the attempt by nation-states to subject data flows to national jurisdictions" [93] as a measure to pursue certain social, political, and economic agendas.[94] Data sovereignty can thus be understood as part of a broader movement within "the Internet's transformation from a technology that resists territorial law to one that facilitates its enforcement."[95]

In India, 'data sovereignty' was popularized by Vinit Goenka, a prominent nationalist politician from the Bharatiya Janata Party (BJP) and the former National Co-Convenor of the Party's IT Cell.[96] On his blog, he defines data sovereignty as something that is an integral part of India's national sovereignty, and that the country's lack of regulations pertaining to data has made "the nation vulnerable in this sphere [cyberspace]."[97] He notes data sovereignty is imperative to avoid a new form of colonisation that exceeds its economic

[91] Couture, Stephane, and Sophie Toupin. "What does the notion of "sovereignty" mean when referring to the digital?." *new media & society* 21, no. 10 (2019): 2305-2322, p. 2319.

[92] DeNardis, Laura. "Hidden levers of Internet control: An infrastructure-based theory of Internet governance." *Information, Communication & Society* 15, no. 5 (2012): 720-738, p. 720.

[93] Polatin-Reuben, Dana, and Joss Wright. "An Internet with {BRICS} Characteristics: Data Sovereignty and the Balkanisation of the Internet." In *4th USENIX Workshop on Free and Open Communications on the Internet.* (2014), p. 1.

[94] Sargsyan, Tatevik. "Data localization and the role of infrastructure for surveillance, privacy, and security." *International Journal of Communication* 10 (2016): 17.

[95] Goldsmith, Jack L. and Wu, Tim. *Who Controls the Internet?: Illusions of a Borderless World* (Oxford: Oxford University Press, 2006), p. 10.

[96] Makhijani, Vishnu. "Data Colonisation the New Looming Danger," Outlook: The News Scroll (Outlook, June 27, 2019), https://www.outlookindia.com/newsscroll/data-colonisation-the-new-looming-danger/1562930.

[97] Goenka, Vinit. "IT SOVEREIGNTY IN INDIA – THE DATA CENTRE DIMENSION," Vinit Goenka , April 11, 2014, https://vinitgoenka.in/it-sovereignty-in-india-the-data-centre-dimension/.

aspects. “Data colonisation” he notes “could lead to the enslavement of mind, body and soul of the affected people.”[98] He asks “[d]on’t you feel overexposed???”[99] especially “considering that 90% of our personal data is stored abroad” and, in a consoling tone, asserts that the “answer lies in enforcing Indian Data to stay in India, in Indian Data Centres, in setups within our borders.”[100] Albeit seemingly exaggerated at first glance, this rhetoric shouldn’t come as a surprise, after all, India too was a target of the data drive manipulations of Cambridge Analytic.[101]

Goenka very well captures the securitizing sentiment in India’s data localisation discourse, speaking of an imminent threat to both the nation and the state that can only be thwarted by implementing a “My Data In My Borders” policy.[102] Additionally, being a technocrat and former Staffing Partner at IBM he employs[103] “techno-utopian solutions.” His rhetoric implying the sense that keeping data within India’s border would somehow be the solution to all its problems. Although they provide great rhetorical fodder that aligns with his nationalist voter base and political peers, they do not necessarily solve the problems that supposedly arise due to a lack of localisation measures. Yet, because it is such a technified field wherein jargon such as “cloud computing services”, “object storage” and “server” are the norm, it is rather difficult for people with a non-technical background to understand, and hence make informed judgements on.[104] The various paradoxes will be discussed in the

[98] Makhijani, Vishnu. “Data Colonisation the New Looming Danger,” Outlook: The News Scroll (Outlook, June 27, 2019), https://www.outlookindia.com/newsscroll/data-colonisation-the-new-looming-danger/1562930.
[99] Goenka, Vinit. “IT SOVEREIGNTY IN INDIA – THE DATA CENTRE DIMENSION,” Vinit Goenka , April 11, 2014, https://vinitgoenka.in/it-sovereignty-in-india-the-data-centre-dimension/.
[100] Ibid.
[101] Aneja, Urvashi. “What Cambridge Analytica Does Is the Norm, Not an Aberration,” Tandem Research, March 23, 2018, https://tandemresearch.org/publications/what-cambridge-analytica-does-is-the-norm-not-an-aberration.
[102] Goenka, Vinit. “IT SOVEREIGNTY IN INDIA – THE DATA CENTRE DIMENSION,” Vinit Goenka , April 11, 2014, https://vinitgoenka.in/it-sovereignty-in-india-the-data-centre-dimension.
[103] Ramanujan-Dixit, Sweta. “From IBM to BJP,” Hindustan Times, August 4, 2008, https://www.hindustantimes.com/india/from-ibm-to-bjp/story-IndtIcA1GxXaQrDHtQJ6AK.html.
[104] Goenka, Vinit. “IT SOVEREIGNTY IN INDIA – THE DATA CENTRE DIMENSION,” Vinit Goenka , April 11, 2014, https://vinitgoenka.in/it-sovereignty-in-india-the-data-centre-dimension.

sections that follow. Ultimately, as appraised by Ranganathan et. al., "data sovereignty in India is a vision created and asserted by arms of the government… and imagines the state as the vessel of such sovereignty."[105]

2.2.2 Foreign surveillance

In line with wanting to have sovereign control of one's data is the argument that data localisation would help avoid foreign transnational surveillance activities. The idea of states wanting to protect data produced therein from the prying eyes of another state gained salience in light of the Snowden revelations which disclosed, among others, how the NSA was able to gain access to the data servers of some of the biggest internet companies like Facebook, Google and Microsoft, and also how the NSA had built surveillance capabilities into internet infrastructure chokepoints to capture vast amounts of internet traffic.[106] As such, the argument goes that physically storing data outside one's jurisdiction makes it less safe, hence the need to localise it. This, however, is flawed because, as has been thoroughly explored by Jennifer Daskal, the "location of access" and the "location of data" need not be the same.[107] The NSA was reported to have a wide arrangement of malicious malware that was able to infiltrate networks across the globe.[108] They supposedly have also tempered with U.S.-made internet routers that allow them backdoor access to the information that flows through them.[109] In the words of one security processional, it suffices to say, within a networked

[105] Kovacs, Anja, and Nayantara Ranganathan. *Data Sovereignty, of Whom? Limits and Suitability of Sovereignty Frameworks for Data in India*. Data Governance Network Working Paper 03. Mumbai, 2019, p. 31.
[106] Chander, Anupam, and Uyên P. Lê. "Data nationalism." *Emory Law Journal* 64 (2014): 677 – 739, p. 714.
[107] Jennifer Daskal, "The Un-Territoriality of Data," Yale Law Journal 125, no. 2 (November 2015): 326-399, p. 369.
[108] "NSA 'Infected' 50,000 Networks with Malware," BBC News (BBC, November 25, 2013), https://www.bbc.com/news/technology-25087627.
[109] Greenwald, Glenn. "How the NSA Tampers with US-Made Internet Routers," The Guardian (Guardian News and Media, May 12, 2014), https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.

world the “only way to really make anything that is NSA [or any other surveillance actress] proof is to not have it connect to the Internet."[110] Finally, data localisation may actually facilitate foreign surveillance efforts by centralizing data.[111]

At the onset of India’s data localisation discourse, the protection against foreign surveillance was one of the main claims put forward by the GoI. The then Deputy National Security Advisor, Nehchal Sandhu, reportedly urged the Department of Telecommunication (DoT) to find ways to route domestic Internet data through servers located in India with the argument that "[s]uch an arrangement would limit the capacity of foreign elements to scrutinize intra-India traffic."[112] This, however, is a questionable argument considering the country’s generally poor track record of avoiding foreign surveillance through digital means. The People’s Republic of China’s, allegedly state-sponsored, operations such as GhostNet, for instance, didn’t rely on technical infrastructure located outside Indian borders but was successful due to India’s poor cybersecurity provisions. [113] The argument of foreign surveillance, nonetheless, soon fell off the priority list for the GoI, with the former external affairs minister Salman Khurshid defending US surveillance efforts by noting “[i]t is only computer analysis of patterns of calls and emails that are being sent. It is not actually snooping on specifically on content of anybody’s message or conversation.”[114] Indeed, it would seem the GoI had quietly launched its similar spying program called the Central

[110] Swartz, Jon. “NSA Surveillance Hurting Tech Firms' Business,” USA Today (Gannett Satellite Information Network, February 28, 2014), https://eu.usatoday.com/story/tech/2014/02/27/nsa-resistant-products-obama-tech-companies-encryption-overseas/5290553/.

[111] Selby, John. "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?." *International Journal of Law and Information Technology* 25, no. 3 (2017): 213-232, p. 228. Chander, Anupam, and Uyên P. Lê. "Data nationalism." *Emory Law Journal* 64 (2014): 677 – 739, p. 714.

[112] Thomas, Thomas K. “Route Domestic Net Traffic via India Servers, NSA Tells Operators,” The Hindu Business Line (The Hindu, March 12, 2018), https://www.thehindubusinessline.com/info-tech/route-domestic-net-traffic-via-india-servers-nsa-tells-operators/article20649047.ece1.

[113] Deibert, Ronald J., Rafal Rohozinski, A. Manchanda, Nart Villeneuve, and G. M. F. Walton. "Tracking ghostnet: Investigating a cyber espionage network." (2009).

[114] “It Is Not Actually Snooping: Khurshid on US Surveillance,” The Hindu (The Hindu, June 4, 2016), https://www.thehindu.com/news/national/it-is-not-actually-snooping-khurshid-on-us-surveillance/article4873351.ece.

Monitoring System(CMS) that “allows authorities to monitor phone calls, texts, and online activities”, which lead to this shift in sentiment.[115] What these contradictions however represent is how a certain threat was constructed, i.e. India’s data as vulnerable to foreign surveillance and consequently a threat to Indian sovereignty and security, thereby justifying the call for data localisation and localized routing, all the while not necessarily making the data any safer from prying eyes.

2.2.3 Security and Privacy

Similar to avoiding foreign surveillance is the claimed goal of protecting the security and privacy of citizen's personal information from non-governmental cyber actresses through data localisation. This is an ironic argument because from a technological standpoint any measures to centralize data actually makes the data less secure.[116] Mandating that all data be stored in one place also makes it more vulnerable in case of software failures or of natural disasters that could be detrimental to its infrastructure. As noted by Daniel Castro, a prominent information technology analyst, “the security of data does not depend on where it is stored, only on the measures used to store it securely.”[117] Considering that global internet companies are subject to intense competition and also have exponentially higher revenues, their security measures tend to be state-of-the-art compared to local storage providers who are protected by the localisation requirements and hence have less incentive to ensure the security of the data.[118] Additionally, they have fewer resources to implement the newest

[115] Nandakumar, Indu. “Government Can Now Snoop on Your SMSs, Online Chats ,” The Times of India, May 7, 2013, https://timesofindia.indiatimes.com/tech-news/government-can-now-snoop-on-your-smss-online-chats/articleshow/19932484.cms.
[116] Reisman, Dillon. “Where Is Your Data, Really?: The Technical Case Against Data Localization,” Lawfare, October 31, 2019, https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization.
[117] Castro, Daniel. “The False Promise of Data Nationalism”, *Information Technology and Innovation Foundation*. No.1 (2013).
[118] Ryan, Patrick S., Sarah Falvey, and Ronak Merchant. "When the cloud goes local: the global problem with data localization." *Computer* 46, no. 12 (2013): 54-59.

security measures.[119] This is what Anupam Chander calls the "Protected Local Provider" problem.[120] Localising data also reduces the opportunity of "sharding."[121] Sharding is the distribution of pieces of a database wherein a "shard" is enough to execute a specific operation but not enough to re-identify an individual.[122] Hindering a distributed data infrastructure hence reduces individual privacy.[123] Ultimately, as observed by numerous computer scientists, it would seem "governments, not private companies, are now emerging as the principal threat to data privacy" and security.[124]

In India, the proposed Personal Data Protection Bill(PDPB) provides one of the central frameworks for data localisation. The formulation of the PDPB was followed by a landmark ruling by the Supreme Court noting that the "Right to Privacy is an integral part of Right to Life and Personal Liberty" thereby confirming privacy as a fundamental right within the Constitution of India.[125] It was in this setting that the Ministry of Electronics & Information Technology (MeitY), to "ensure [the] growth of the digital economy while keeping personal data of citizens secure and protected", mandated a "Committee of Experts to deliberate on a data protection framework for India."[126] Led by retired Supreme Court Judge Justice B. N. Srikrishna the Committee was comprised of professionals of various fields including notable computer scientists such as the Director of Indian Institute of Technology Bhilai (IIT) Rajat Moona, and Dr. Ajay Bhushan Pandey, also a graduate from the IIT, the report has become the blueprint for the current PDPB.

[119] Ibid.
[120] Chander, Anupam, and Uyên P. Lê. "Data nationalism." *Emory Law Journal* 64 (2014): 677 – 739, p. 719.
[121] Ryan, Patrick S., Sarah Falvey, and Ronak Merchant. "When the cloud goes local: the global problem with data localization." *Computer* 46, no. 12 (2013): 54-59.
[122] Ibid.
[123] Ibid.
[124] Ibid, p. 58.
[125] Mahapatra, Dhananjay and Choudhary, Amit Anand. "Supreme Court: Right to Privacy Is a Fundamental Right, It Is Intrinsic to Right to Life: India News - Times of India," The Times of India (Times of India, August 24, 2017), https://timesofindia.indiatimes.com/india/right-to-privacy-is-a-fundamental-right-supreme-court/articleshow/60203394.cms.
[126] "Constitution of Committee of Experts to deliberate on a data protection framework for India," Ministry of Electronics and IT, 31st July, 2017, Government of India.

Titled, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians", the report certainly sounds like a noble project at first glance. Yet, it and consequently the PDBP has been muddled with criticisms. In an open letter by a number of notable citizens including government officials and various civil and digital rights organizations, the group voiced its concerns about the "non-transparency" and "inadequate representation" of the Committee and called "for public consultation for wider input."[127] After all, they note "understanding of the impact of policy will necessitate the inclusion of civil society members who have been examining the impact of such initiatives on democratic rights. This includes matters of privacy, surveillance, aggregation of data, the commercial collection of data and its use and, more broadly, data used to restrict constitutional and other rights."[128] In reference to the Supreme Court ruling mentioned above, the group had highlighted how some in the Committee had actually "taken stands …[that]challenge the fundamental right to privacy", hence contradicting the purpose of them being in the Committee in the first place.[129] Furthermore, they note, "[M]ost members on the current committee have in the past voiced or echoed views that seem to support Aadhaar."[130] Indeed, it would seem that the same Dr. Pandey mentioned above is the CEO of the Unique Identification Authority of India (UIDAI aka. Aadhaar).[131]

This is an important detail because India's Aadhaar initiative has been in the limelight of privacy concerns.[132] In comparison to other national identification registries such as the US Social Security Number for instance, with Aadhaar citizens "biometric and demographic

[127] Chishti, Seema. "Eminent Citizens Write to the Committee of Experts on Data Protection Framework," The Indian Express, November 6, 2017, https://indianexpress.com/article/india/citizens-group-questions-data-privacy-panel-composition-aadhaar-4924220/.
[128] Ibid.
[129] Ibid.
[130] Ibid.
[131] Ibid.
[132] Khera, Reetika. "The Different Ways in Which Aadhaar Infringes on Privacy," The Wire, July 19, 2017, https://thewire.in/government/privacy-aadhaar-supreme-court.

data are…stored in a centralised database."[133] Further, every dataset is associated with a unique identifier which is "sought to be 'seeded' (added as a new data field) with every possible – public and private – database in the country."[134] It is in this context that the country's proposal to localize data becomes concerning. After all, if Facebook (or any other internet company for that matter) were to store its data in India, through Aadhaar's unique identifier a "bridge across the hitherto disconnected data silos" can be built thereby allowing the government to create extremely comprehensive profiles of its citizens.[135] Indeed, as noted by Jean Drèze, simply the possibility of such profiling would lead to self-censorship and stifle dissent.[136] In any case, the group's concern regarding the Committee "mostly fell on deaf ears", as reported by the Internet Freedom Foundation (IFF)[137] and when concerns regarding data privacy and security are raised they are often "obfuscated" by the government. In conversation with Dr. Panday, the CEO of Aadhaar, he assures that "[n]o one can build Aadhaar users' profile."[138] Yet, as reported by Reetika Khera, a Professor at IIT Delhi, "he misinterprets profiling. What he is actually talking about is 'identity fraud', rather than profiling in the civil liberties sense."[139] Indeed, this highlights that as a technical expert, individuals such as Dr. Panday can transcend topics that are deemed political because they and their opinions are widely understood to be technical and thereby non-partisan.

2.2.4 Local law enforcement and content regulation

[133] Ibid.
[134] Ibid.
[135] Ibid.
[136] Dreze, Jean. "Dissent and Aadhaar," The Indian Express, May 8, 2017, https://indianexpress.com/article/opinion/columns/dissent-and-aadhaar-4645231/.
[137] Kaur, Sukhnidh. "#StartFromScratch: The Data Bill Series, Part 1!," Internet Freedom Foundation (Internet Freedom Foundation, March 26, 2021), https://internetfreedom.in/startfromscratch-the-data-bill-series-part-1/.
[138] Khera, Reetika. "The Different Ways in Which Aadhaar Infringes on Privacy," The Wire, July 19, 2017, https://thewire.in/government/privacy-aadhaar-supreme-court.
[139] Ibid.

In line with having sovereign control over the data produced within one's jurisdiction, governments argue for data localisation to ease access for local law enforcement agencies and also for content regulation in the midst of increasing online disinformation.[140] Since governments not only have a right but also a responsibility to protect their citizens, this is certainly a legitimate argument. This argument is bolstered when considering the exponential increase in cybercrime[141], rampant fake news[142] , and sophistication of terrorist activities.[143] The concern, however, is the fine line between judicious law enforcement, surveillance, and censorship. Although data localisation may improve the effectiveness of law enforcement and increase the government's control over data, it certainly also has the potential to amplify its surveillance and censorship efforts threatening the human rights of its citizenry. Tatevik Sargsyan, in exploring the political nature of internet infrastructure, for instance, argues that calls to localise data by state actresses are measures to "configure intermediaries' private infrastructure for their political goals."[144] Since information intermediaries the likes of Facebook and Google are generally subject to laws wherein they have physical operations,[145] countries that host their data centers "have more opportunities to exercise influence over companies' decisions and claim jurisdiction over data stored in their territory."[146] On the other hand, this makes one wonder why Mutual Legal Assistance Treaties (MLATs) [147] with

[140] Chander, Anupam, and Uyên P. Lê. "Data nationalism." *Emory Law Journal* 64 (2014): 677 – 739, p. 730.
[141] Broadhurst, Roderic, and Lennon YC Chang. "Cybercrime in Asia: trends and challenges." In *Handbook of Asian criminology*, pp. 49-63. Springer, New York, NY, 2013.
[142] Das, Anupam, and Ralph Schroeder. "Online disinformation in the run-up to the Indian 2019 election." *Information, Communication & Society* (2020): 1-17.
[143] Derrick, DC, GS Ligon, M. Harms, and W. Mahoney. "Cyber-Sophistication Assessment Methodology for Public-Facing Terrorist Web Sites." *Journal of Information Warfare* 16, no. 1 (2017): 13-30.
[144] Sargsyan, Tatevik. "Data localization and the role of infrastructure for surveillance, privacy, and security." *International Journal of Communication* 10 (2016): 17, p. 2223.
[145] Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world.* Oxford, UK: Oxford University Press.
[146] Sargsyan, Tatevik. "Data localization and the role of infrastructure for surveillance, privacy, and security." *International Journal of Communication* 10 (2016): 17, p. 2224.
[147] Chander, Anupam, and Uyên P. Lê. "Data nationalism." *Emory Law Journal* 64 (2014): 677 – 739, p. 7333.

foreign nations are not enhanced especially considering the high economic costs to localizing data[148] and the potential data security risks.[149]

In India, law enforcement's access was expressed as one of the primary reasons to localize data. The Sri Krishna report noted that the "requirement to store personal data locally would boost law enforcement efforts to access information… because it is easier for law enforcement agencies to access information within their jurisdiction."[150] Indeed, the local storage of data is argued to be inherently connected to the enforcement of domestic laws.[151] This view is also supported by key individuals in the country such as Kiran Vasireddy, the CEO of Paytm, a major e-commerce payments provider, who notes the "moment data leaves the country, it falls under various jurisdictions" hence is "is important to keep all the data here so that the laws of the land can be made applicable to them."[152] While this may be true, especially considering that it takes at least 10 months to obtain data from US service providers through MLAT[153], a lack in privacy provisions and the increasingly repressive nature of the current administration[154], however, make the true intentions rather questionable. After all, as noted above, if data access to law enforcement is truly a major concern, why not find ways to enhance the MLATs. This sentiment is reflected in a piece by G. Mahith Vidya Sagar, an Advocate for the High Court in Andhra Pradesh, who concludes by asserting that India's "current legal infrastructure has lacunas to resolve certain legal issues that will be

[148] Bauer, Matthias, Hosuk Lee-Makiyama, Erik Van der Marel, and Bert Verschelde. *The costs of data localisation: Friendly fire on economic recovery*. No. 3/2014. ECIPE Occasional Paper, 2014.
[149] Komaitis, Konstantinos. "The 'wicked problem'of data localisation." *Journal of Cyber Policy* 2, no. 3 (2017): 355-365, p. 359.
[150] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians," Ministry of Electronics and IT, 27th July, 2018, Government of India, p. 88.
[151] Ibid, p. 87.
[152] Khatri, Bhumika. "Paytm Continues To Support Data Localisation, Mirroring Data Not The Solution," Inc42 Media, July 24, 2018, https://inc42.com/buzz/paytm-continues-to-support-data-localisation-mirroring-data-not-the-solution/.
[153] Swire, Peter, DeBrae Kennedy-Mayo, and Arjun Jayakumar. "India's Access to Criminal Evidence in the US: A Proposed Framework for an Executive Agreement," ORF Special Report No. 123, December 2020, Observer Research Foundation.
[154] Vij, Shivam. "Why the Modi Government Gets Away with Lies, and How the Opposition Could Change That," ThePrint, May 15, 2020, https://theprint.in/opinion/why-modi-government-gets-away-with-lies/422211/.

posed by the data localisation."[155] These lacunas include for instance the vagueness of what is meant by "critical personal data" that is mandated to be stored in India under the PDPB and the largely unfettered access GoI agencies will have to it.[156]

To garner a more holistic understanding of the data localisation provisions in India one should also look at them in relation to other policies, such as the IT Rules (Guidelines For Intermediaries And Digital Media Ethics Code) 2021. Indeed, it has been reported that in combination with the PDPB they "will determine how the internet and internet-based companies function in the country in future" and also "regulate what you can or cannot do, see or access through internet. In essence, they will determine the future of the internet in India."[157] While these new IT measures were passed to place a degree of accountability on intermediary platforms such as Facebook and Twitter especially in light of rampant disinformation and fake news, the clause on traceability is of particular concern because it mandates that law enforcement be able to trace "the first originator of the information."[158] The worry here is that it would hurt user privacy guaranteed by the end-to-end encryption offered by messaging services such as WhatsApp. As one spokesperson notes, implementing this requirement means "asking us (i.e. WhatsApp or any other messaging service that provides end-to-end encryption) to keep a fingerprint of every single message sent."[159]

[155] Vidyasagar, G. Mahith, Advocate High Court of Andhra Pradesh.. "Does Data Localisation Measure Really Enhance Law Enforcement?" Humanities Commons. NyaayShastra Law Review, Volume II Issue I (May 2021), p. 15.
[156] Garg, Rohin. "#DataProtectionTop10: Data Localisation," Internet Freedom Foundation (Internet Freedom Foundation, May 21, 2021), https://internetfreedom.in/dataprotectionttop10-data-localisation-a-threat-to-free-and-open-internet/.
[157] Banerjee, Prasid. "How New IT Rules Will Change the Internet in India," mint, February 28, 2021, https://www.livemint.com/news/india/how-new-it-rules-will-change-the-internet-in-india-11614532759640.html.
[158] Dhapola, Shruti. "Explained: WhatsApp's Arguments to Fight Traceability Clause in IT Rules 2021," The Indian Express, June 2, 2021, https://indianexpress.com/article/explained/whatsapp-india-it-rules-traceability-clause-case-explained-7331039/.
[159] Ibid.

Consequently, WhatsApp has sued the GoI because such laws are “unconstitutional and against people’s fundamental right to privacy.”[160]

While one of the primary drafters of the law, Rakesh Maheshwari, a graduate of the Delhi College of Engineering and one of the leading computer security experts in the country assures that the rules will not be used to break end-to-end encryption[161], other non-governmental parties have asserted that such provisions are an “onerous obligation that severely undermines end-to-end encryption.”[162] The point of the matter is that because it is so-called technical experts leading the conversation they often (in)advertently miss how certain provisions on technology may affect society adversely because they concentrate on the technical aspects of a certain issue. Secondly, because it has to do with technical nitty-gritties only a handful of people can be a part of the conversation, hence one is more or less forced to place blind trust in these individuals. After all, how does one confirm whether or not the traceability clause actually breaks end-to-end encryption and thereby undermines user privacy? Indeed, this is technification at its best because “[t]echnical as encryption can be, it is really about something at the very core of how we live our lives today: Should people be able to have a private conversation when they are not together in person?”[163] Yet, unless these technicalities are explained in a matter that is understandable to the wider public, it remains out of the purview of a wider debate.

2.2.5 Economic argument

[160] Ibid.

[161] “Meity Says Intermediary Guidelines Will Not Be Used to Break Encryption - ET Telecom,” ETTelecom (The Economic Times, May 7, 2021), https://telecom.economictimes.indiatimes.com/news/meity-says-data-protection-rules-will-not-be-used-to-break-encryption-of-intermediaries/82455481.

[162] Bansal, Varsha. “WhatsApp's Fight With India Has Global Implications,” Wired (Conde Nast), accessed June 3, 2021, https://www.wired.com/story/whatsapp-india-traceability-encryption/.

[163] Cathcart, Will. “Encryption Has Never Been More Essential-or Threatened,” Wired (Conde Nast, May 4, 2021), https://www.wired.com/story/opinion-encryption-has-never-been-more-essential-or-threatened/.

Data localisation is often also argued in terms of economic development; that it would increase investment, create new jobs and enhance the growth of local businesses. This, however, is a flawed argument on few accounts. Firstly, unless localizing data within a specific country significantly raises the economic benefits for a particular firm, it is unlikely that such an investment will occur. Especially considering the cost “to maintain servers in each of the countries in which they do business, rather than in a single location.”[164] Secondly, data centres are essentially just pieces of technology in a warehouse that mostly run autonomously hence once construction is completed the scope for new employment opportunities remains limited.[165] Thirdly, local data centres may have higher costs than ones abroad which enjoy economies of scale and may have more favourable operating conditions such as cheaper electricity, hence raising the costs for local business.[166] Furthermore, data localisation initiatives may even lead to exclusions from global services thereby hindering local productivity and innovation while incurring high economic costs.[167] The economic argument is closely linked to the fear that foreign firms are exploiting citizen's data in a new form of colonialism called data colonialism.[168] While this is a valid argument considering the booming data economy in the U.S. for instance, such fears could more efficiently be combated through provisions that require user consent and or stricter guidelines on how such data may be processed.[169]

[164] Komaitis, Konstantinos. "The ‘wicked problem’of data localisation." *Journal of Cyber Policy* 2, no. 3 (2017): 355-365, p. 361.
[165] Hardy, Quentin. “Cloud Computing Brings Sprawling Centers, but Few Jobs, to Small Towns,” The New York Times (The New York Times, August 26, 2016), https://www.nytimes.com/2016/08/27/technology/cloud-computing-brings-sprawling-centers-but-few-jobs-to-small-towns.html?_r=1.
[166] Selby, John. "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?." *International Journal of Law and Information Technology* 25, no. 3 (2017): 213-232, p. 229.
[167] Bauer, Matthias, Hosuk Lee-Makiyama, Erik Van der Marel, and Bert Verschelde. *The costs of data localisation: Friendly fire on economic recovery*. No. 3/2014. ECIPE Occasional Paper, 2014.
[168] Couldry, Nick, and Ulises A. Mejias. "Data colonialism: Rethinking big data’s relation to the contemporary subject." *Television & New Media* 20, no. 4 (2019): 336-349.
[169] Ibid.

The idea of data being a national resource that India must capitalize on is certainly one of the main arguments presented by the GoI for its data localisation provisions. In the Sri Krishna report, there is a particular focus on the value that artificial intelligence will bring to all sectors of the economy, citing how China's focus on AI would add "1.6 percentage points to China's economic growth."[170] The report notes the "growth of AI is heavily dependent on harnessing data" hence the need for "policies that would ensure the processing of data within the country using local infrastructure built for that purpose."[171] Further, based on a study by Azmeh and Foster[172], the report asserts, data localisation will firstly lead to higher "foreign direct investment in digital infrastructure" and secondly foster a domestic market for data centres through job creation, "enhanced connectivity and presence of skilled professionals."[173] Such claims, however, not only contradict the literature referenced above, but also an extensive report that analysed the impacts of data localisation for India by CUTS international, a well-established NGO focusing on equality, equity, and social justice for consumers[174], which concludes that "[i]f data is localised, innovation will go down, costs will increase, and technology opportunities will decrease."[175] This is also reflected in a report by the Internet and Mobile Association of India (IAMAI) that noted, data localisation "would reduce competitiveness and would have a deterring impact on the GDP."[176]

Indeed, what this contradiction highlight's is that the economic argument presented has less to do with the economic empowerment of its 1.3 billion citizens who are generating

[170] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians," Ministry of Electronics and IT, 27th July, 2018, Government of India, p. 91.
[171] Ibid, p. 92.
[172] Azmeh, Shamel and Christopher Foster. "The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements*," London School of Economics Working Paper* No. 16-175, (2016), p. 26-27.
[173] Ibid, p. 92.
[174] CUTS International, "Vision and Mission," https://cuts-international.org/vision-mission/
[175] Gupta, Shagufta, Kapil Gupta, Poulomi Ghosh, and Sudip Kumar Paul. "Data Localisation: India's Double Edged Sword?." *CUTS International (2020),* p. 45.
[176] "Make in india: Conducive policy and regulatory environment to incentivise data center infrastructure." *Internet and Mobile Association of India.* (2016).

the data, but more to do with the potential benefits of a select few within the private and public sector. After all, as noted by Pradip Thomas, a particular feature of "the neo-liberal State in India is that it has become thoroughly 'marketized', perhaps best illustrated by the fact that the Digital India project is based on public-private partnership (PPP) in which private firms are closely involved in shaping India's digital future."[177] This becomes even more apparent considering the primary actresses calling for the data to be localised using securitising imageries of India's colonial experience that must not be repeated. The Reliance Chairman and also the country's richest man, Mukesh Ambani, for instance, noted "Gandhi led a political movement against political colonisation. Today, we have to collectively launch a new movement against data colonisation."[178] He calls data the "new oil" and the "new wealth" of the 21st century and hence should be "controlled and owned by Indian people and not by corporates, especially global corporations."[179] As such, in addressing the PM he notes, "I am sure you will make this [ending data colonisation] one of the principal goals of your Digital India mission."[180] Considering that Jio, one of the numerous enterprises under the Reliance empire, has over a third of Indian citizens (i.e. over 300 million people) as its customers and consequently the largest telecom service provider in the country, there is no doubt that individuals such as Mukesh Ambani have a lot to gain from data localisation measures.[181] Jio is, after all, set to become Microsoft's largest partner globally and plans to build "data centres across India, consisting of next-generation computer, storage, and

[177] Thomas, Pradip Ninan. *The Politics of Digital India: Between Local Compulsions and Transnational Pressures*. Oxford University Press, 2019, p. 9.
[178] "India's Data Must Be Controlled by Indians: Mukesh Ambani," mint, January 19, 2019, https://www.livemint.com/Companies/QMZDxbCufK3O2dJE4xccyI/Indias-data-must-be-controlled-by-Indians-not-by-global-co.html.
[179] Ibid.
[180] Ibid.
[181] "Reliance Jio Partners Microsoft for Cloud Infrastructure," BusinessLine (The Hindu , August 12, 2019), https://www.thehindubusinessline.com/info-tech/rjio-microsoft-sign-10-year-deal-for-cloud-infrastructure/article29005535.ece#:~:text=On%20Monday%2C%20during%20Reliance%20Industry's,the%20cloud%2Dbased%20collaboration%20tools.

networking capabilities" to deploy Microsoft's "Azure platform."[182]A similar scenario can be noticed with Gautam Adani, "India's infrastructure king" and second richest man in the country, who recently signed an agreement with EdgeConneX, one of the world's leading data centre providers.[183]

While there is certainly nothing wrong with companies like Jio willing to make a profit as such, it does become problematic considering their businesses are increasingly based on behavioural modifications and the capitalisation of people's data through indiscriminate tracking, capturing, storing, and processing.[184] Big data analytics has, after all, become Reliance Jio's "bulwark for market share expansion."[185] In their analysis of India's draft e-Commerce Policy, paradoxically subtitled "India's Data for India's Development", Nayantara Ranganathan from the Internet Democracy Project eloquently highlights this paradox, claiming that in the "name of enabling the country to benefit from rapid digitalization of the economy, the policy enables large scale extraction of data, while imagining frameworks like that of data protection to be models that legitimise such extraction instead of protecting against them."[186] Furthermore, the concern is compounded when these companies say they will share said data with the government. Indeed, Jio and Paytm have both been reported to agree to law enforcement's access to data including "decryption keys to sensitive and personal data of citizens."[187] In the view of Mishi Choudhary, a prominent technology

[182] Ibid.
[183] "India's Infrastructure King: Adani Sees World's Top Wealth Surge," Business and Economy News (Al Jazeera, March 25, 2021), https://www.aljazeera.com/economy/2021/3/25/bb-indiasinfrastructureking-adani-sees-worlds-top-wealth-surge.
[184] Zuboff, Shoshana. "Big other: surveillance capitalism and the prospects of an information civilization." *Journal of Information Technology* 30, no. 1 (2015): 75-89.
[185] Bhatia, Richa. "Is Big Data Turning the Wheels at Reliance Jio – inside the Youngest Mobile Operator's Big Data Strategy," Analytics India Magazine, August 7, 2017, https://analyticsindiamag.com/big-data-turning-wheels-reliance-jio-inside-youngest-mobile-operators-big-data-strategy/.
[186] Ranganathan, Nayantara. "Submission in Response to the Draft e-Commerce Policy," Internet Democracy Project, April 1, 2019, https://internetdemocracy.in/policy/submission-in-response-to-the-draft-e-commerce-policy.
[187] Sathe, Gopal. "Reliance Jio, Paytm Tell TRAI They Will Spy on Us For The Government," HuffPost India (HuffPost, January 29, 2019), https://www.huffpost.com/archive/in/entry/reliance-jio-paytm-tell-trai-the-government-should-be-able-to-access-your-data_in_5c4f30e9e4b0f43e4109647c.

lawyer, and social activist, “the Indian tech business works like [a] traditional business, they’re not looking to disrupt things unlike the valley [i.e. Silicon Valley], they just want to add new players to the old game.”[188]

Here the conversation isn’t technified per se, the importance of data is primarily framed as a national resource that needs to be capitalised on, through imageries of a colonial past that must not be repeated. Such populist rhetoric certainly serves to gain wide support, especially under the current nationalist BJP administration, yet the crux of the matter, i.e. precisely how data localisation will lead to economic empowerment, and to whose, is not a conversation at all. This is because the field itself is technical and technified. How is the normal individual supposed to understand the intricacies of surveillance capitalism for instance?

Chapter 3: India’s “Digital Strike”

3.1 Brief history of India-China Relations

The 1st of April 2021 marked the 71st anniversary of the establishment of diplomatic relations between India and China. While the early years of this relationship were rather cordial amounting to "Hindi Chini Bhai Bhai" (India and China are brothers), the war of 1962 and subsequent annexation of Aksai Chin by China planted the seeds of mistrust between the two nations.[189] Rajiv Gandhi’s visit to the PRC in December 1988, however, set the stage for a new modus operandi with Deng Xiaoping and saw the resumption of trade, relaxation on travel restrictions, confidence-building initiatives in the border areas, normalization in military relations, and an increase in

[188] Ibid.
[189] Vijay Gokhale, “The Road from Galwan: The Future of India-China Relations,” March 10, 2021, https://carnegieindia.org/2021/03/10/road-from-galwan-future-of-india-china-relations-pub-84019.

multilateral cooperation.[190] Indeed, the ensuing two decades were largely frictionless and mutually beneficial as both countries' power and role in the international arena grew. Nonetheless, cracks started to emerge in the mid-to-late 2000s as China, inter alia, halted the Line of Actual Control (LAC) clarification exercises, continued its sale of lethal weapons to Pakistan, and the GhostNet malware was uncovered, while India, among other activities, has rebuffed China's Belt and Road Initiative, unilaterally revoked the special status of Jammu and Kashmir, and has become an increasingly close ally of the United States following Obama's 'pivot to Asia' foreign policy.[191]

3.2 India bans apps that are "Prejudicial to Sovereignty and Integrity of India"

The cracks ultimately culminated into violent border skirmishes at the Galwan Valley on June 15th, tumbling India-China relations to the lowest they've been in 45 years.[192] Following the death of 20 Indian soldiers, the pressure was mounting for the GoI to act. Consequently, in a move that sends a clear message, the Indian administration launched a "digital strike."[193] On June 29th, by invoking the controversial section 69 of the IT Act[194], the MeitY announced the ban of 59 mobile apps including the likes of TikTok and WeChat, "since in view of [the] information available they [the banned apps] are engaged in activities which is prejudicial to sovereignty and integrity of India,

[190] Ibid.
[191] Ibid.
[192] Snehesh Alex Philip, "Why the Remote Galwan Valley Is a Flashpoint between India and China," ThePrint, June 16, 2020, https://theprint.in/defence/why-the-remote-galwan-valley-is-a-flashpoint-between-india-and-china/442794/
[193] Tripathi, Ashutosh. "'Banning Chinese Apps a Digital Strike': Union Minister Ravi Shankar Prasad," Hindustan Times, July 2, 2020, https://www.hindustantimes.com/india-news/banning-chinese-apps-a-digital-strike-union-minister-ravi-shankar-prasad/story-XQQbTVt4bauqeBHfXC75iM.html.
[194] Deol, Taran. "All about Section 69A of IT Act under Which Twitter Had Withheld Several Posts & Accounts," ThePrint, February 2, 2021, https://theprint.in/theprint-essential/all-about-section-69a-of-it-act-under-which-twitter-had-withheld-several-posts-accounts/597367/.

defence of India, security of state and public order."[195] This clearly exemplifies a case of securitisation. The apps, which facilitate the flow of data out of the territorial bounds of India, are deemed to be threatening the security and sovereignty of India, therefore the necessity to ban them (thereby halting the flow of data), hence restoring the country's security and sovereignty. Indeed, as the *communiqué* asserts, it "is a matter of very deep and immediate concern which requires emergency measures"[196], employing a rhetoric of an existential and imminent threat.

The notice further claims,

> At the same time, there have been raging concerns on aspects relating to data security and safeguarding the privacy of 130 crore Indians…The Ministry of Information Technology has received many complaints from various sources including several reports about misuse of some mobile apps…for stealing and surreptitiously transmitting users' data in an unauthorized manner to servers which have locations outside India.[197]

The vagueness of the statements, the lack of references to the supposed excess of concerns, and the absence of any reports that explain how and in what ways these apps are allegedly being misused in ways that are threatening to India, further serve to support the state of securitisation.

Additionally, by linking the threat to individual Indians and their privacy, a second referent object is constructed that speaks to the audience of the securitising actor i.e. the Indian population. Indeed, by linking one's data, one's privacy, one's online experience to imageries of war by popularising the app ban as a "digital strike" by prominent members of the ruling BJP party facilitates the intersubjective agreement that allows for securitisation to

[195] "Government Bans 59 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order," Press Information Bureau (Ministry of Electronics & IT, June 20, 2020), https://pib.gov.in/PressReleseDetail.aspx?PRID=1635206.
[196] Ibid.
[197] Ibid.

happen. The app ban is ultimately framed as a measure that "will safeguard the interests of crores of Indian mobile and internet users."[198]

Finally, the claim that the flow of data to servers located outside of India was illegal, is contradictory too. After all, at the time of this statement and presently, India does not have any laws on the localisation of data generated by social media apps like TikTok. The Personal Data Protection Bill (PDPB), discussed in the previous section, is yet to be passed into law. However, because a state of heightened security was created, the issue is taken out of what would be considered "normal" politics, consequently reducing the space for political, media, and public scrutiny of this policy. This sentiment is reflected by individuals such as by Apar Gupta, a lawyer and Director for the Internet Freedom Foundation, who, in light of further bans in September and November[199] 2020 with the same justifications, lamented "[t]he kind of power being used with these bans, there's no degree of transparency."[200]

The official communication by MeitY then mobilises technification through vague technical jargon that further obfuscates the matter. They claim, "[t]he compilation of these data, its mining and profiling by elements hostile to national security and defence of India…ultimately impinges upon the sovereignty and integrity of India."[201] Terms and concepts such as data mining, data compilation, or data profiling, however, only mean anything to someone working in that industry. Unless one is for instance an information scientist or a computer expert or a professional working in the field of cybersecurity, one is limited in comprehending what is meant and hence unable to make an informed judgment or partake in any manner of deliberations. After all, if technical issues are not framed in a

[198] Ibid.
[199] "Government Bans 43 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order," Press Information Bureau (Ministry of Electronics & IT, November 24, 2020), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1675335.
[200] Dhapola, Shruti. "More Chinese Apps Banned in India: Lack of Transparency Is Worrying, Say Experts," The Indian Express, November 26, 2020, https://indianexpress.com/article/technology/tech-news-technology/more-chinese-apps-banned-in-india-lack-of-transparency-is-worrying-say-experts/.
[201] Ibid.

manner that is understandable to the general population the democratic process cannot function properly. Additionally, the lack of technical details allows for the banning of apps that are wildly different and seemingly arbitrary. Indeed, the apps that have been banned range from TrulyAsian, an Asian dating app, to AliExpress, an e-commerce app, to Baidu Maps which is a web mapping service application.[202] As Manish Tewari, a politician from the opposition Congress party, asks in a tweet, "why is Alibaba [a Chinese conglomerate that has reportedly invested over $2 billion in Indian companies][203] not on the ban list?... With this ban are you also certifying that other Chinese APP's are not a security threat ?"[204] This arbitrariness highlights the constructed nature of the threat. Ultimately, the securitisation of Indian cyberspace is maintained through this process of technification because it further reduces the scrutinising threshold of the app ban policy.

Conclusion

This thesis explored the various paradoxes of data localisation by taking India as its case study. As such, building upon Copenhagen School's securitisation theory and the concept of technification as developed the Hansen and Nissenbaum, the thesis appraised the sophistries in the arguments provided by the GoI towards implementing data localisation policies through a discourse analysis. The GoI argues that it wants to have sovereign control of the data generated and flowed within its borders, to circumvent foreign surveillance, to promote the security and privacy of its citizen's data, to alleviate law enforcement's access to

[202] "Government Bans 59 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order," Press Information Bureau (Ministry of Electronics & IT, June 20, 2020), https://pib.gov.in/PressReleseDetail.aspx?PRID=1635206.

[203] Shah, Aditi and Chatterjee, Sumeet. "Exclusive: Alibaba Puts India Investment Plan on Hold amid China Tensions, Sources Say," Reuters (Thomson Reuters, August 26, 2020), https://www.reuters.com/article/us-alibaba-india-investment-exclusive-idUSKBN25M200.

[204] Tewari, Manish. Tweet (June 30, 2020). https://twitter.com/ManishTewari/status/1277803920711016448?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1277803920711016448%7Ctwgr%5E%7Ctwcon%5Es1_c10&ref_url=https%3A%2F%2Fwww.republicworld.com%2Findia-news%2Fpolitics%2Fcongs-manish-tewari-questions-ban-on-chinese-apps-says-its-symbolic.html

data stored in other jurisdictions, and to boost the domestic economy and foster data-driven innovation, yet the analysis showed that far from fulfilling such goals, the conversation is dominated by technical experts who (in)advertently stifle public deliberations due to the technical nature of data localisation and how it could potentially have adverse consequences. Furthermore, by deconstructing India's "digital strike" that banned dozens of apps that were deemed a threat to the security and sovereignty of India, the thesis exemplified how data localisation was used as a securitising move to securitise, or in the words of MietY "ensure safety, security and sovereignty of Indian cyberspace."[205] In appraising the official statement issued by MietY, the thesis noted the mobilisation of technification by highlighting the use of technical terms and concepts that was vague insubstantial. Consequently, in seeking to answer what the role of data localisation is in the securitisation of cyberspace, it argued that data localisation is itself a securitising move facilitated through technification.

Concludingly, this study highlighted that although data localisation efforts are framed as a measure that protects and empowers Indian citizens by keeping their data within India, the reality is quite different. In an environment where WhatsApp is suing the GoI for violating its privacy provisions by mandating that the messaging service be able to trace the originator of a certain message, to a rising number of Twitter account suspensions, to an arbitrary banning of apps, it would seem data localisation measures essentially increases the government's surveillance and censorship efforts while a few in the private sector make huge financial gains for building the infrastructure. Indeed, it would seem that Modi and the current administration would rather be on top of the clouds instead of being 'hovered' by them.

[205] "Government Bans 43 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order," Press Information Bureau (Ministry of Electronics & IT, November 24, 2020), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1675335.

Bibliography

Al Jazeera "India's Infrastructure King: Adani Sees World's Top Wealth Surge," Business and Economy News (Al Jazeera, March 25, 2021), https://www.aljazeera.com/economy/2021/3/25/bb-indiasinfrastructureking-adani-sees-worlds-top-wealth-surge.

Aneja, Urvashi. "What Cambridge Analytica Does Is the Norm, Not an Aberration," Tandem Research, March 23, 2018, https://tandemresearch.org/publications/what-cambridge-analytica-does-is-the-norm-not-an-aberration.

Azmeh, Shamel and Christopher Foster. "The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements*," London School of Economics Working Paper* No. 16-175, (2016).

Balzacq, Thierry, Sarah Léonard, and Jan Ruzicka. "'Securitization'revisited: Theory and cases." *International Relations* 30, no. 4 (2016): 494-531.

Banerjee, Prasid. "How New IT Rules Will Change the Internet in India," mint, February 28, 2021, https://www.livemint.com/news/india/how-new-it-rules-will-change-the-internet-in-india-11614532759640.html.

Bansal, Varsha. "WhatsApp's Fight With India Has Global Implications," Wired (Conde Nast), accessed June 3, 2021, https://www.wired.com/story/whatsapp-india-traceability-encryption/.

Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." *Electronic Frontier Foundation.* https://www.eff.org/cyberspace-independence.

Basu, Arindrajit et. al., *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India* (Pranav M Bidrae et. al. eds., The Centre for Internet Society, Mar. 19, 2019).

Bauer, Matthias, Hosuk Lee-Makiyama, Erik Van der Marel, and Bert Verschelde. *The costs of data localisation: Friendly fire on economic recovery*. No. 3/2014. ECIPE Occasional Paper, 2014.

BBC, "NSA 'Infected' 50,000 Networks with Malware," BBC News (BBC, November 25, 2013), https://www.bbc.com/news/technology-25087627.

Bhatia, Richa. "Is Big Data Turning the Wheels at Reliance Jio – inside the Youngest Mobile Operator's Big Data Strategy," Analytics India Magazine, August 7, 2017, https://analyticsindiamag.com/big-data-turning-wheels-reliance-jio-inside-youngest-mobile-operators-big-data-strategy/.

Bigo, Didier. *"Security and immigration: Toward a critique of the governmentality of unease."* Alternatives 27, no. 1_suppl (2002): 63-92.

Broadhurst, Roderic, and Lennon YC Chang. "Cybercrime in Asia: trends and challenges." In *Handbook of Asian criminology*, pp. 49-63. Springer, New York, NY, 2013.

Business Today “India's Decision to Allow 5G Trials without Huawei, ZTE a Sovereign Step: US,” Business Today, May 12, 2021, https://www.businesstoday.in/current/economy-politics/india-decision-to-allow-5g-trials-without-huawei-zte-a-sovereign-step-us/story/438830.html.

Business Today, “India's Digital Strike on China: After Chinese Apps' Ban, Govt Trains Guns on Fintech Firms,” Business Today, September 22, 2020, https://www.businesstoday.in/current/corporate/indias-digital-strike-on-china-chinese-apps-ban-fintech-firms-on-govts-radar-mobile-based-lenders/story/416687.html.

Butler, Judith. 2009. *Frames of War: When Is Life Grievable?* London: Verso, 2009. xiii.

Buzan, Barry, and Lene Hansen. *The evolution of international security studies*. Cambridge University Press, 2009.

Buzan, Barry, Ole Wæver and Jaap De Wilde. *Security: A new framework for analysis*. Lynne Rienner Publishers, 1998.

Castro, Daniel. “The False Promise of Data Nationalism”, *Information Technology and Innovation Foundation*. No.1 (2013).

Cathcart, Will. “Encryption Has Never Been More Essential-or Threatened,” Wired (Conde Nast, May 4, 2021), https://www.wired.com/story/opinion-encryption-has-never-been-more-essential-or-threatened/.

Chander, Anupam, and Uyên P. Lê. "Data nationalism." *Emory Law Journal* 64 (2014): 677 – 739.

Chishti, Seema. “Eminent Citizens Write to the Committee of Experts on Data Protection Framework,” The Indian Express, November 6, 2017, https://indianexpress.com/article/india/citizens-group-questions-data-privacy-panel-composition-aadhaar-4924220/.

Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, “A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians,” Ministry of Electronics and IT, 27th July, 2018, Government of India.

Couldry, Nick, and Ulises A. Mejias. "Data colonialism: Rethinking big data’s relation to the contemporary subject." *Television & New Media* 20, no. 4 (2019): 336-349.

Couture, Stephane, and Sophie Toupin. "What does the notion of “sovereignty” mean when referring to the digital?." *new media & society* 21, no. 10 (2019): 2305-2322, p. 2319.

CUTS International, “Vision and Mission,” https://cuts-international.org/vision-mission/

D.K. Singh, “Between Vajpayee and Modi Era, RSS Has Learnt Many Political Lessons,” ThePrint, February 22, 2021, https://theprint.in/opinion/politically-correct/between-vajpayee-and-modi-era-rss-has-learnt-many-political-lessons/609419/.

Das, Anupam, and Ralph Schroeder. "Online disinformation in the run-up to the Indian 2019 election." *Information, Communication & Society* (2020): 1-17.

Deibert, Ronald J., Rafal Rohozinski, A. Manchanda, Nart Villeneuve, and G. M. F. Walton. "Tracking ghostnet: Investigating a cyber espionage network." (2009).

DeNardis, Laura. "Hidden levers of Internet control: An infrastructure-based theory of Internet governance." *Information, Communication & Society* 15, no. 5 (2012): 720-738.

Deol, Taran. “All about Section 69A of IT Act under Which Twitter Had Withheld Several Posts & Accounts,” ThePrint, February 2, 2021, https://theprint.in/theprint-essential/all-about-section-69a-of-it-act-under-which-twitter-had-withheld-several-posts-accounts/597367/.

Derrick, DC, GS Ligon, M. Harms, and W. Mahoney. "Cyber-Sophistication Assessment Methodology for Public-Facing Terrorist Web Sites." *Journal of Information Warfare* 16, no. 1 (2017): 13-30.

Dhapola, Shruti. “Explained: WhatsApp's Arguments to Fight Traceability Clause in IT Rules 2021,” The Indian Express, June 2, 2021, https://indianexpress.com/article/explained/whatsapp-india-it-rules-traceability-clause-case-explained-7331039/.

Dhapola, Shruti. “More Chinese Apps Banned in India: Lack of Transparency Is Worrying, Say Experts,” The Indian Express, November 26, 2020, https://indianexpress.com/article/technology/tech-news-technology/more-chinese-apps-banned-in-india-lack-of-transparency-is-worrying-say-experts/.

Digital India, “Digital India is a flagship programme of the Government of India with a vision to transform India into a digitally empowered society and knowledge economy.” https://www.digitalindia.gov.in/

Dreze, Jean. “Dissent and Aadhaar,” The Indian Express, May 8, 2017, https://indianexpress.com/article/opinion/columns/dissent-and-aadhaar-4645231/.

ETTelecom, “Meity Says Intermediary Guidelines Will Not Be Used to Break Encryption - ET Telecom,” ETTelecom (Economic Times Telcom, May 7, 2021), https://telecom.economictimes.indiatimes.com/news/meity-says-data-protection-rules-will-not-be-used-to-break-encryption-of-intermediaries/82455481.

Foroohar, Rana. “The Internet Splits Up,” Newsweek, March 13, 2010, https://www.newsweek.com/internet-splits-110491.

Garg, Rohin. “#DataProtectionTop10: Data Localisation,” Internet Freedom Foundation (Internet Freedom Foundation, May 21, 2021), https://internetfreedom.in/dataprotectionttop10-data-localisation-a-threat-to-free-and-open-internet/.

Goenka, Vinit. “IT SOVEREIGNTY IN INDIA – THE DATA CENTRE DIMENSION,” Vinit Goenka , April 11, 2014, https://vinitgoenka.in/it-sovereignty-in-india-the-data-centre-dimension.

Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world.* Oxford, UK: Oxford University Press.

Greenwald, Glenn. “How the NSA Tampers with US-Made Internet Routers,” The Guardian (Guardian News and Media, May 12, 2014), https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.

Gupta, Charu. "Hindu women, Muslim men: Love Jihad and conversions." *Economic and Political Weekly* (2009): 13-15.

Gupta, Shagufta, Kapil Gupta, Poulomi Ghosh, and Sudip Kumar Paul. "Data Localisation: India's Double Edged Sword?." *CUTS International* (2020).

Hansen, Lene, and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." *International studies quarterly* 53, no. 4 (2009): 1155-1175.

Hardy, Quentin. “Cloud Computing Brings Sprawling Centers, but Few Jobs, to Small Towns,” The New York Times (The New York Times, August 26, 2016), https://www.nytimes.com/2016/08/27/technology/cloud-computing-brings-sprawling-centers-but-few-jobs-to-small-towns.html?_r=1.

Hinrich Foundation and All India Management Association, (2019)*, The Data Opportunity: The Promise of Digital Trade for India.* https://alphabeta.com/wp-content/uploads/2019/08/digitrade_india.pdf

Huysmans, Jef. *The politics of insecurity: Fear, migration and asylum in the EU*. Routledge, 2006.

IAMAI, “Make in india: Conducive policy and regulatory environment to incentivise data center infrastructure.” *Internet and Mobile Association of India.* (2016).

Jennifer Daskal, "The Un-Territoriality of Data," Yale Law Journal 125, no. 2 (November 2015): 326-399.

Kaur, Sukhnidh. “#StartFromScratch: The Data Bill Series, Part 1!,” Internet Freedom Foundation (Internet Freedom Foundation, March 26, 2021), https://internetfreedom.in/startfromscratch-the-data-bill-series-part-1/.

Khatri, Bhumika. “Paytm Continues To Support Data Localisation, Mirroring Data Not The Solution,” Inc42 Media, July 24, 2018, https://inc42.com/buzz/paytm-continues-to-support-data-localisation-mirroring-data-not-the-solution/.
Khera, Reetika. “The Different Ways in Which Aadhaar Infringes on Privacy,” The Wire, July 19, 2017, https://thewire.in/government/privacy-aadhaar-supreme-court.

Komaitis, Konstantinos. "The ‘wicked problem’of data localisation." *Journal of Cyber Policy* 2, no. 3 (2017): 355-365.

Kovacs, Anja, and Nayantara Ranganathan. *Data Sovereignty, of Whom? Limits and Suitability of Sovereignty Frameworks for Data in India*. Data Governance Network Working Paper 03. Mumbai, 2019.

Kremer, Jan-Frederik, and Benedikt Müller, eds. *Cyberspace and international relations: Theory, prospects and challenges*. Springer Science & Business Media, 2013, 66.

Léonard, Sarah. "EU border security and migration into the European Union: FRONTEX and securitisation through practices." *European security* 19, no. 2 (2010): 231-254.

Live Free or Die Hard (2007) - Theatrical Trailer [HD]. https://www.youtube.com/watch?v=8Jz-8UcCiws&t=48s

Live Mint, “India's Data Must Be Controlled by Indians: Mukesh Ambani,” mint, January 19, 2019, https://www.livemint.com/Companies/QMZDxbCufK3O2dJE4xccyI/Indias-data-must-be-controlled-by-Indians-not-by-global-co.html.

Mahapatra, Dhananjay and Choudhary, Amit Anand. “Supreme Court: Right to Privacy Is a Fundamental Right, It Is Intrinsic to Right to Life: India News - Times of India,” The Times of India (Times of India, August 24, 2017), https://timesofindia.indiatimes.com/india/right-to-privacy-is-a-fundamental-right-supreme-court/articleshow/60203394.cms.

Makhijani, Vishnu. “Data Colonisation the New Looming Danger,” Outlook: The News Scroll (Outlook, June 27, 2019), https://www.outlookindia.com/newsscroll/data-colonisation-the-new-looming-danger/1562930.

McStay, Andrew. "I consent: An analysis of the Cookie Directive and its implications for UK behavioral advertising." *New Media & Society* 15, no. 4 (2013): 596-611.

MietY, “Constitution of Committee of Experts to deliberate on a data protection framework for India,” Ministry of Electronics and IT, 31st July, 2017, Government of India.

MietY, “Government Bans 43 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order,” Press Information Bureau (Ministry of Electronics & IT, November 24, 2020), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1675335.

MietY, “Government Bans 59 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order,” Press Information Bureau (Ministry of Electronics & IT, June 20, 2020), https://pib.gov.in/PressReleseDetail.aspx?PRID=1635206.

Nandakumar, Indu. “Government Can Now Snoop on Your SMSs, Online Chats ,” The Times of India, May 7, 2013, https://timesofindia.indiatimes.com/tech-news/government-can-now-snoop-on-your-smss-online-chats/articleshow/19932484.cms.

Nissenbaum, Helen. "Where Computer Security Meets National Security." In *Cybercrime*, pp. 59-84. New York University Press, 2007.

Our Bureau, “Reliance Jio Partners Microsoft for Cloud Infrastructure,” BusinessLine (The Hindu , August 12, 2019), https://www.thehindubusinessline.com/info-tech/rjio-microsoft-sign-10-year-deal-for-cloud-infrastructure/article29005535.ece#:~:text=On%20Monday%2C%20during%20Reliance%20Industry's,the%20cloud%2Dbased%20collaboration%20tools.

Pohle, Julia, and Thorsten Thiel. "Digital sovereignty." *Internet Policy Review* 9, no. 4 (2020).

Polatin-Reuben, Dana, and Joss Wright. "An Internet with {BRICS} Characteristics: Data Sovereignty and the Balkanisation of the Internet." In *4th USENIX Workshop on Free and Open Communications on the Internet.* (2014).

Ramanujan-Dixit, Sweta. “From IBM to BJP,” Hindustan Times, August 4, 2008, https://www.hindustantimes.com/india/from-ibm-to-bjp/story-IndtIcA1GxXaQrDHtQJ6AK.html.

Ranganathan, Nayantara. “Submission in Response to the Draft e-Commerce Policy,” Internet Democracy Project, April 1, 2019, https://internetdemocracy.in/policy/submission-in-response-to-the-draft-e-commerce-policy.

Reisman, Dillon. “Where Is Your Data, Really?: The Technical Case Against Data Localization,” Lawfare, October 31, 2019, https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization.

Ryan, Patrick S., Sarah Falvey, and Ronak Merchant. "When the cloud goes local: the global problem with data localization." *Computer* 46, no. 12 (2013): 54-59.

Safi, Michael. “India Election Results 2019: Modi Claims Landslide Victory,” The Guardian (Guardian News and Media, May 23, 2019), https://www.theguardian.com/world/2019/may/23/india-election-results-narendra-modi-bjp-victory.

Sahgal, Priya. “Decoding Data Sovereignty: The Pursuit of Supremacy, Cover Story Special,” YouTube (NewsX, June 10, 2019), https://www.youtube.com/watch?v=RVB8UapHvdQ&t=300s.

Sargsyan, Tatevik. "Data localization and the role of infrastructure for surveillance, privacy, and security." *International Journal of Communication* 10 (2016): 17.

Sathe, Gopal. “Reliance Jio, Paytm Tell TRAI They Will Spy on Us For The Government,” HuffPost India (HuffPost, January 29, 2019), https://www.huffpost.com/archive/in/entry/reliance-jio-paytm-tell-trai-the-government-should-be-able-to-access-your-data_in_5c4f30e9e4b0f43e4109647c.

Selby, John. "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?." *International Journal of Law and Information Technology* 25, no. 3 (2017): 213-232.

Shah, Aditi and Chatterjee, Sumeet. “Exclusive: Alibaba Puts India Investment Plan on Hold amid China Tensions, Sources Say,” Reuters (Thomson Reuters, August 26, 2020), https://www.reuters.com/article/us-alibaba-india-investment-exclusive-idUSKBN25M200.

Snehesh Alex Philip, “Why the Remote Galwan Valley Is a Flashpoint between India and China,” ThePrint, June 16, 2020, https://theprint.in/defence/why-the-remote-galwan-valley-is-a-flashpoint-between-india-and-china/442794/

Statista, “Number of internet users in India from 2015 to 2020 with a forecast until 2025.” https://www.statista.com/statistics/255146/number-of-internet-users-in-india/

Strizel, H. (2007). Towards a Theory of Securitization: Copenhagen and Beyond. European Journal of International Relations 13(3): 357–383.

Swartz, Jon. “NSA Surveillance Hurting Tech Firms' Business,” USA Today (Gannett Satellite Information Network, February 28, 2014), https://eu.usatoday.com/story/tech/2014/02/27/nsa-resistant-products-obama-tech-companies-encryption-overseas/5290553/.

Swire, Peter, DeBrae Kennedy-Mayo, and Arjun Jayakumar. "India’s Access to Criminal Evidence in the US: A Proposed Framework for an Executive Agreement," ORF Special Report No. 123, December 2020, Observer Research Foundation.

Tewari, Manish. Tweet (June 30, 2020). https://twitter.com/ManishTewari/status/1277803920711016448?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1277803920711016448%7Ctwgr%5E%7Ctwcon%5Es1_c10&ref_url=https%3A%2F%2Fwww.republicworld.com%2Findia-news%2Fpolitics%2Fcongs-manish-tewari-questions-ban-on-chinese-apps-says-its-symbolic.html

The Hindu, “It Is Not Actually Snooping: Khurshid on US Surveillance,” The Hindu (The Hindu, June 4, 2016), https://www.thehindu.com/news/national/it-is-not-actually-snooping-khurshid-on-us-surveillance/article4873351.ece.

The Hindu, “World Facing 'Bloodless' Cyber War Threat: Modi,” The Hindu (The Hindu, April 1, 2016), https://www.thehindu.com/news/national/world-facing-bloodless-cyber-war-threat-modi/article7375190.ece.

The Terminator (1984) Official Trailer. https://www.youtube.com/watch?v=k64P4l2Wmeg

Thomas, Pradip Ninan. *The Politics of Digital India: Between Local Compulsions and Transnational Pressures*. Oxford University Press, 2019.

Thomas, Thomas K. “Route Domestic Net Traffic via India Servers, NSA Tells Operators,” The Hindu Business Line (The Hindu, March 12, 2018), https://www.thehindubusinessline.com/info-tech/route-domestic-net-traffic-via-india-servers-nsa-tells-operators/article20649047.ece1.

Tripathi, Ashutosh. “'Banning Chinese Apps a Digital Strike': Union Minister Ravi Shankar Prasad,” Hindustan Times, July 2, 2020, https://www.hindustantimes.com/india-news/banning-chinese-apps-a-digital-strike-union-minister-ravi-shankar-prasad/story-XQQbTVt4bauqeBHfXC75iM.html.

Vidyasagar, G. Mahith, Advocate High Court of Andhra Pradesh.. “Does Data Localisation Measure Really Enhance Law Enforcement?” Humanities Commons. NyaayShastra Law Review, Volume II Issue I (May 2021).

Vij, Shivam. “Why the Modi Government Gets Away with Lies, and How the Opposition Could Change That,” ThePrint, May 15, 2020, https://theprint.in/opinion/why-modi-government-gets-away-with-lies/422211/.

Vijay Gokhale, “The Road from Galwan: The Future of India-China Relations,” March 10, 2021, https://carnegieindia.org/2021/03/10/road-from-galwan-future-of-india-china-relations-pub-84019.

Vultee, Fred. "Securitization: A new approach to the framing of the “war on terror”." *Journalism practice* 4, no. 1 (2010): 33-47.

Zuboff, Shoshana. "Big other: surveillance capitalism and the prospects of an information civilization." *Journal of Information Technology* 30, no. 1 (2015): 75-89.