The Balkanisation of the Internet: Data Nationalism in the European Union and its Effects on the Development of Technology

LL.M. Law and Technology
Tilburg Institute for Law, Technology, and Society, Tilburg University
Nwachukwu T. Obi II
Snr 2048416
January 2022

Supervisor: Dr. Emmanuel Pernot-Leplay
Second Reader: Dr. Bo Zhao

Table of Contents

Table of Contents ..... **iii**
Dedication ..... **v**
Acknowledgement ..... **vi**
Chapter I – Introduction **1**
1.1. Background 1
1.2. Objective and research questions 3
1.3. Significance 3
1.4. Preliminary remarks and scope of the research 4
1.5. Literature review 4
1.6. Methodology 5
1.7. Chapter overview 5
Chapter II – Scope and Extent of Data Nationalism **6**
2.1. Introduction 6
2.2. Why data nationalism is increasing 6
2.3. Data nationalism distinguished from data sovereignty 8
2.3.1. Justifications and challenges for data nationality 10
2.4. Different forms of data nationalism 11
2.5. Conclusion 15
Chapter III – The Legal Framework Governing Data Nationalism **17**
3.1.Introduction 17
3.2.Data Nationalism in the EU 17
3.2.1. Transfers or disclosures not authorised by Union law 19
3.2.2. Derogations for specific situations 21
3.3. Data nationalism in the People's Republic of China 21
3.3.1. Concepts of ‘personal information’ and ‘important data’ 22
3.3.2. PRC's data localisation requirements 24
3.3.3. Cross-border data transfer requirements in the PRC 25
3.4. Reconciling the provisions 25
3.5. Conclusion 26
Chapter IV-A Global data protection agreement as a possible way forward **28**
4.1. Introduction 28
4.2.Data nationalism and the Balkanisation of the Internet 28
4.3.The Balkanisation of the Internet and the economy 29
4.4.The Balkanisation of the Internet and human rights concerns 31
4.5. The Balkanisation of the Internet and the new surveillance state 33
4.6. The way forward 35
4.7. Accommodating data nationalism 36
4.8. Feasibility of a multilateral agreement to circumvent hard data nationalism 36
4.9. Essential aspects of a multilateral agreement 37
4.9.1. Conditions for transferring data 38
4.9.1.1. Restriction of data localisation 38
4.9.1.2. Prior judicial review 38
4.9.2. Data subject rights and effective judicial remedies 39
4.10. Conclusion 39
Chapter V-Conclusion 41
Bibliography 45
Primary Sources 45

Secondary Sources 46

Dedication

This Thesis is dedicated to the memory of the Late Chief Tonye Willie-Harry, *Dein na sime* Grandpa

Acknowledgement

My Appreciation, first of all, goes to Almighty God, with whom everything is possible. My sincere thanks and honour to my dear parents, Chris and Telema Obi, who have been a source of motivation, provision and inspiration to me over the past year. Their love and guidance have contributed immensely to the successful completion of this body of work.

I would like to express my gratitude to my supervisors Dr. Emmanuel Pernot-Leplay and Dr. Bo Zhao LLM, for their detailed and vastly enriching recommendations, guidance and tutelage to the content and structure of this thesis. My amazing siblings, Ibifaa, Nkili and Omiete, thank you for believing in me even when I didn't believe in myself. Those weekend conversations gave me a reason to go on when it felt like I was not going to complete this thesis on time.

I am grateful to my dear friends for their love, care and help over the past couple of years that culminated in this body of work. Mukhtar, Bidemi, Timi, Poju, Daniel, Wale, Akanbi, Sukkie, Jhoe, Bolu, Kaykay, Yemi, Toyosi, Yeni, Oprah, Osa, Ibrahim, Monsuratu, and Ken, you have all contributed one way or another to this body of work by listening to my rantings on my ideas and just being there for me. Thank you for the support, love and care.

Furthermore, my immense appreciation goes to the Willie-Harry, Bamboshe, Shofela, Adejuyigbe, Adesunkanmi, Omidiran, Oyewo, Paramole, Ajogwu and Kenna Partners families for their kindness and support over the years. Moving to a new country undoubtedly poses unique challenges, and I am grateful to Dieye Willie Harry and his beautiful family, the beautiful people of Talent Square Flat 443 and our Bulgarian and International cohorts, Franklyn, Idopikhin, and Stephanie, for cushioning the effect of the move to a new country. I will also like to acknowledge many unnamed friends and colleagues who have provided valuable moral support, guidance, a listening ear, good memories, and significant interactions over the years and during this Master's degree. Thank You!

Finally, I would like to thank Manchester United for again having a slump in the past couple of months that gave me all the free time I needed to focus on this task at hand.

It has been quite a journey, and here we are at the conclusion, all done! Baby steps do not mean you are not moving. Just keep moving!

Nwachukwu Obi II

January, 2022

Chapter I – Introduction

1.1. Background

The digital age has brought a renewed sense of globalism and togetherness amongst countries as respective power blocks. This togetherness has now given way, and the Internet as we know it is being splintered based on geography for a host of reasons. This division raises several pertinent legal and policy concerns. Initially, governments all struggled to manage and understand new innovative technology that heralded the rise of the Internet.[1] During that discovery period, there was cooperation amongst most nations and open-source sharing mechanisms to develop what is now known as the global digital economy.[2]

Most of the digital developments that led to the rise of the Internet and the global digital economy were built through the use and harvesting of big data. Over time, the impact of big data on the hyperconnected growth of the digital economy ecosystem was so significant and valuable that big data became a valuable resource and became known as the new 'oil,' i.e., one of the most valuable resources to be analysed and exploited.[3] When the time came, most of these countries even took hints to regulate innovative technology.[4] However, the mutual openness that came with the free Internet has now ended. Countries developed rapid policy changes as they understood the proprietary nature and myriad uses of personal data.

Additionally, the Edward Snowden whistleblowing incident in 2013 and the Cambridge Analytica scandal in 2017 raised suspicions on the use of proprietary data by corporations and even countries. As a result, the various countries that came together to make the Internet a global borderless phenomenon now adopt a more nativist and nationalist stance to the use of their data and technology. The United States of America's threats to ban or nationalise the Chinese social media application *Tik Tok* in the United States as a result of concerns of users' data security by the Chinese government is a watershed instance whereby nativist steps were taken to protect data supremacy. Another notable instance is the decision of the European Court of Justice in *Schrems II*,[5] whereby the EU-USA data privacy shield was struck down as a result of concerns that the American law enforcement agencies will exploit data of European residents without following due procedures. Various nations and tech power blocks have erected what can be called digital barriers that will effectively lead to what is now known as data nationalism.

Today, the interconnectivity of the digital era may be over, with countries like The United States of America (US), The United Kingdom (UK), the People's Republic of China

---

[1] Sylvia Ostry, Richard R. Nelson, Techno-Nationalism and Techno-Globalism: Conflict and Cooperation page 3 (Brookings Institution Press, 1995) ISBN: 9780815766735

[2] Don Tapscott, 'The Digital Economy: 20th Anniversary Edition' 449.at page 16

[3] Ibrar Yaqoob and others, 'Big Data: From Beginning to Future' (2016) 36 International Journal of Information Management 1231 <https://linkinghub.elsevier.com/retrieve/pii/S0268401216304753> accessed 14 May 2021.

[4] Olga Petricevic and David J Teece, 'The Structural Reshaping of Globalization: Implications for Strategic Sectors, Profiting from Innovation, and the Multinational Enterprise' (2019) 50 Journal of International Business Studies at 1488 <http://link.springer.com/10.1057/s41267-019-00269-x> accessed 14 May 2021.

[5] Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, Case C-311/18

(PRC),[6] India, Russia, Malaysia, the United Arab Emirates, and the European Union[7] are all taking hard-line stances on the nationalism of data through various stringent means.[8]

Additionally, the European Union (EU) is a power block and policy forerunner in technology regulation that adopts a human rights approach to utilising data involving natural persons in the EU.[9] As a result of those differences, all these power blocs have gone about creating enormous digital 'walls' through stringent transfer laws around the data concerning their citizens to further their agendas.[10]

Consequently, the global legal framework on data nationalism is disjointed with many different points of interest, especially concerning data protection and privacy, surveillance, censorship, transparency, digital money, and intellectual property.[11] This will effectively render the transfer of data nearly impossible in the future and lead to the end of the Internet as we currently know it. Thus, the competing ideologies could potentially splinter the newfound global Internet system in ways not seen since the Cold War's peak.[12] This splinter is called the Balkanisation of the Internet, and it raises several extensive reservations on the freedom of information, right to free speech, censorship, freedom of trade and commerce.

While Balkanisation is an old and familiar phrase coined in a New York Times interview with German politician Walther Rathenau in 1918,[13] the term 'Balkanisation of the Internet' has held different meanings at different times to various scholars since the advent of the Internet. Its current meaning pejoratively describes a rising threat to the Internet's status as a borderless globe-spanning network popularised by Scott Malcomson.[14] Thus, it is essential that while addressing data concerns, the policies espoused do not lead to the Internet's splintering.

---

[6] 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)' Article 37 (New America) <http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/> accessed 16 August 2021.

[7] For instance, 'Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data | European Data Protection Board' <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en> accessed 16 August 2021. Point to increased support for additional data nationalism measures within the EU.

[8] Nigel Cory, 'The False Appeal of Data Nationalism: Why the Value of Data Comes From How It's Used, Not Where It's Stored' at 14.

[9] David D'Hollander, Axel Marx and Jan Wouters, 'Integrating Human Rights in EU Development Cooperation Policy: Achievements and Challenges' [2014] at 4, 5 and 6 SSRN Electronic Journal <http://www.ssrn.com/abstract=2431190> accessed 16 May 2021.

[10] Victoria Higgins, 'The Perils of Strategic Technological Development Policy: Two Failed Chinese Attempts, FDI and Techno-Nationalism' in Victoria Higgins (ed), Alliance Capitalism, Innovation and the Chinese State: The Global Wireless Sector (Palgrave Macmillan UK 2015) <https://doi.org/10.1057/9781137529657_2>.

[11] Alex Capri, 'Techno-nationalism: The US-China tech innovation race, New challenges for markets, business and academia', Hinrich Foundation, (2020) page 5

[12] David E.H. Edgerton, 'The Contradictions of Techno-Nationalism and Techno-Globalism: A Historical Perspective', New Global Studies, Volume 1, Issue 1 (2007) Article 1-

[13] Mariiã Nikolaeva Todorova, Imagining the Balkans (Updated ed, Oxford University Press 2009). Page 33

[14] Scott Malcomson, 'Welcome to the SplInternet' (Techonomy, 22 December 2015) <https://techonomy.com/2015/12/welcome-to-the-splInternet/> accessed 16 August 2021; SCOTT MALCOMSON, SplInternet (OR Books 2016) <http://www.jstor.org.tilburguniversity.idm.oclc.org/stable/j.ctt20bbwp4> accessed 16 August 2021.

1.2. Objective and research questions

The primary focus of this research will be directed towards reviewing the existing legal perspective on the European Union policies with regards to data nationalism within the context of the increasing fears in the further Balkanisation of the Internet. Over the course of this research, detailed reference will be made to China's data nationalism legislation and policies, as the PRC is one of the first nations that has splintered itself from the global Internet. It is also one of the first nations to take data nationalism seriously as a digital policy.[15] Additionally, reference will be made to issues on the restriction of data transfers and access to data in the European Union. This issue has a literature gap that will be fulfilled with this research.

Hence, the thesis will answer the following **main research question**:

> *How do data nationalism laws affect concerns on the Balkanisation of the Internet?*

In order to answer the central research question, the following **sub-questions** are to be dealt with:

1. *Can the European Union adopt data nationalism policies for its Member States?*
2. *How does the European Union, through the General Data Protection Regulation and other relevant European laws, nationalise data?*
3. *How are concerns on the Balkanisation of the Internet exacerbated by data nationalism?*
4. *What are feasible solutions for the conflict discussed under sub-question three, and what are the requirements in terms of necessary safeguards that must be considered?*

1.3. Significance

Since the enactment of the GDPR,[16] and all the additional regulations and case law on the expanding scope of data and data transfers, the EU increasingly finds itself trapped in a quagmire getting data out of the EU. They are confronted with seemingly constricting legal obligations, without any option for acting in accordance with EU law. When one considers that these policies were enacted to protect EU residents or the national security of EU states, and juxtaposes this fact with the need for a free and open Internet and global access to information, the need for a detailed analysis of the conflict, and the need for possible solutions seem compelling.

However, it is of utmost importance that any such solutions raised, the protection of the fundamental right to data protection under the European legal framework, is not undermined. Hence, this thesis will play a role in exploring and proposing the necessary

---

[15] Haiping Zheng, 'Regulating the Internet: China's Law and Practice' (2013) 04 Beijing Law Review 37 at 6 <http://www.scirp.org/journal/doi.aspx?DOI=10.4236/blr.2013.41005> accessed 14 May 2021; 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)' (n 14).

[16] 'EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1'. (General Data Protection Regulation (GDPR)) <https://gdpr-info.eu/> accessed 27 August 2021.

safeguards that must be included in applying and creating data nationalism policies to prevent the further Balkanisation of the Internet.

1.4. Preliminary remarks and scope of the research

The scope of this thesis focuses on the consequences on foreign businesses with a presence in the EU and the free one Internet as a result of the laws and regulations in the EU mandating data nationalism. The converse way of European businesses with a global presence addressing issues of data nationalism will not be analysed in detail. Furthermore, this thesis will address the issue primarily from a personal data protection perspective. Hence, legal questions regarding cybercrime and eCommerce will only be touched upon to the extent necessary to answer the research questions.

1.5. Literature review

Due to the fact that data nationalism is an ongoing issue within the tech world, it has many specific problems connected with national security and international trade. Several assumptions have been made on the subject by researchers and institutions following:

The current literature available around the subject of data nationalism is focused on either its geopolitical aspects as Chander and Lê's detailed analysis[17] and how it affects political and economic relations of regions once the policies are in place, or on ethical challenges such as addressing privacy concerns as Pernot-LePlay's middle-out strategy targets.[18]

The majority of research papers found address general privacy issues that arise as a result of this practice, but most of them do not specifically address the concerns in national security, localisation, and transfer, as well as the concerns that arise from the adoption of these policies and how to adequately address them, especially within in the context of the peculiarities of the European Union. Additionally, the fact that the Personal Information Protection Law of the People's Republic of China (PIPL) is very recently passed means it has not been analysed, thereby identifying a gap in the literature.

Some researchers such as Cory[19] have taken the first steps in raising awareness about the severe general impact that data nationalism can have on the global Internet, pointing to some concerns, including a stifling of innovation and an increase in global distrust. Hence, the research papers selected analyse the concepts of 'data nationalism'. Additionally, Bauer and Lee-Makiyama have analysed the technical aspects of data transfers, and localisation has helped reach the focus of this research thesis.[20]

---

[17] Chander. A & Uyên P. Lê, 'Data Nationalism', 64 Emory L. J. (2015) at 680- ; Bagchi, Kaushambi; Kapilavai, Sashank, ''Political Economy of Data Nationalism', (22nd Biennial Conference of the International Telecommunications Society (ITS), June 2018)-'.

[18] Emmanuel Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?' 71.

[19] Cory (n 8).

[20] Anupam Chander, 'Is Data Localization a Solution for Schrems II?' 15; Matthias Bauer and Hosuk Lee-Makiyama, 'The Costs Of Data Localısatıon: Frıendly Fıre On Economıc Recovery' at 20; Helena Ursic and others, 'Data Localisation Measures and Their Impacts on Data Science', Research Handbook in Data Science and Law (Edward Elgar Publishing 2018) at 322 <https://www.elgaronline.com/view/edcoll/9781788111294/9781788111294.00021.xml>; 'Data Localization

1.6. Methodology

This thesis is primarily based on doctrinal legal research on statutory legislation, case law, and academic literature on data protection law. The research will be done within the context of criminal law, health law, privacy law, and e-commerce directives in the EU regarding China's position. The research will critically review those aforementioned laws within the context of erecting digital barriers to the transfer of personal data to third countries.

An in-depth legal analysis of the relevant provisions of the GDPR, alongside the existing legislations on restrictions in transfer, storage, and processing of data in the EU within distinct sectors, will be conducted, and it will be examined whether the policies will lead to additional splintering up of the Internet. Moreover, relevant provisions of the recently passed Data Security Law of the People's Republic of China (DSL), The Personal Information Protection Law of the People's Republic of China (PIPL), and the Cyber Security Law of the People's Republic of China CSL) will be explored and critically evaluated.

Recent legal initiatives in the European legal framework will be assessed when elaborating an alternative solution. The primary focus will be directed to create proposals to address the Balkanisation of the Internet concerns that data nationalism raises.

1.7. Chapter overview

This thesis will be structured in the following way: After the Introduction (2), the detailed scope of data nationalism with a classification of the phenomenon into different forms and detailed analysis into each form and how it affects concerns of the Balkanisation of the Internet will be analysed (3). The following chapter will review the current legal framework within which data nationalism works in the EU. The Chinese legal framework on the localisation, storage, and data transfers will also be evaluated. Both frameworks will be compared, contrasted, juxtaposed, and analysed to understand how they may affect concerns of the Balkanisation of the Internet (4). Afterwards, the limitations data nationalism raises, especially within the concept of the current debate on the Balkanisation of the Internet, will be illustrated, and the conflict between the data nationalism and the one Internet ideal will be explicated. Assessment of a possible solution to the established conflict in the scope of an international agreement between the EU, the PRC and the US, and the appropriate safeguards for such an agreement will be compiled. Ultimately, based on the result of the previous chapters, the conclusion will recapitulate the legal conflict, explicate to what extent relaxed policies could serve as a solution, and summarise the necessary safeguards in the form of recommendations.

and the Limits of 'Everything from Everywhere'' (JD Supra) <https://www.jdsupra.com/legalnews/data-localization-and-the-limits-of-5695264/> accessed 16 August 2021.

Chapter II – Scope and Extent of Data Nationalism

2.1. Introduction

This chapter will evaluate the meaning and scope of data nationalism within the EU and Chinese legal and political systems. Afterwards, this chapter will illustrate the limitations data nationalism raises, especially within the concept of the current debate on the Balkanisation of the Internet. Additionally, the research in this chapter will explicate the conflict between data nationalism and the one Internet ideal.

In order to establish the legal and policy dilemma that underlies this thesis, it is essential first to explore the concepts being discussed and their background exhaustingly. To this end, this chapter will first present and discuss key concepts. Afterwards, this chapter will examine the legal questions raised by data transfers in the EU. Furthermore, case law like Schrems I and Schrems II that focuses on the reasons for the restriction of data transfers will be analysed in addition to the implication of that decision to the US-EU privacy shield.

2.2. Why data nationalism is increasing

Over the past few years, the importance of protecting data subjects from abuse and manipulation has been at the frontline in deciding international policy on technology. This has become more important when considering that people generate 2.5 quintillion bytes of data globally.[21] Additionally this global data generation is projected to elevate to 175 zettabytes (ZB) by 2025 (175,000,000,000,000,000,000,000 bytes).[22] That figure represents a whopping 61% year-on-year Compound Annual Growth Rate.[23] Furthermore, 51% of that data generated will be stored in data centres worldwide, while the remaining 49% will be housed using cloud storage. 90 ZB of this data will come from the Internet of Things (IoT) devices in 2025, including wearables like watches and household appliances like refrigerators and even printers, as opposed to simply personal computers and smartphones. [24]Furthermore, International Data Corporation estimates that by 2025 at least 46% of the total stored data globally will be resident in public cloud environments.[25]

The above statistics have highlighted just how vital data is to the world today. As a result of all that data being churned out and processed, the issue of protecting that data adequately has arisen. To this end, the term data nationalism is often quoted as one of the solutions to the problems raised by technology. However, the term 'data nationalism' is not used consistently in all the related discussions.

One very general definition refers to it as 'a policy whereby national governments compel Internet content hosts to store data about Internet users in their country on servers

---

[21] Andy Patrizio, 'IDC: Expect 175 Zettabytes of Data Worldwide by 2025' (Network World, 3 December 2018) 5 <https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html> accessed 27 October 2021.

[22] Patrizio (n 21).

[23] ibid.

[24] ibid.

[25] 'Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts' (IDC: The premier global market intelligence company) <https://www.idc.com/getdoc.jsp?containerId=prUS47560321> accessed 27 October 2021.

located within the jurisdiction of the government'.[26] A clear definition of the data categories and the techniques concerned would be essential to address the potential limitations of data nationalism policies based on other legal frameworks, particularly data protection rules.[27]

According to Anupam Chander and Uyê P. Lê, data nationalism refers to measures that specifically encumber the transfer of data across municipal borders.[28] These measures take a wide variety of forms – including rules preventing information from being sent outside the country; rules requiring the prior consent of the data subject before the information is transmitted across national borders; rules requiring copies of information to be stored domestically, and even a tax on the export of data.[29] Chander and Lê believe that data localisation and data nationalism are two concepts that can be interchanged. For the context of this thesis, the terms will be treated as interchangeable, with data localisation being a form of data nationalism. The merging of the concepts brings value to this discussion because it enables data nationalism to be analysed from a point of view that is not restricted. The forms of data nationalism will be examined further in detail within this chapter.

The definition raises several crucial concerns, the largest of which is the somewhat convoluted categories of state actions that count as data nationalism. Additionally, the definition raises concerns about whether data can be subject to nationalism in the EU because this research hinges on the possibility that data can be nationalised. This question is increased because the EU is made up of twenty-seven distinct nations, each with its unique laws and national policies. Some countries in the European Economic Area are not part of the European Union, such as Norway and the United Kingdom. Thus, it is difficult for data policies to be nationalistic for an economic block that is not a nation but is made up of countries. The EU states adopt a relatively uniform approach to data protection with particular distinctions when necessary.

Additionally, there are relatively consistent laws and a shared Court of Justice for the European Economic Area and the wider European continent. Thus, the GDPR, Council of Europe Treaty 108,[30] and the unique set of regulations it creates points to an almost uniform approach to data protection by the EU Member States. Many EU Member States have localised the GDPR or similar data protection policies culled from the GDPR.[31] Some of those states' positions will be mentioned, when necessary, in the analysis of data nationalism. Although it generally seems that the conversation on data privacy is steered mainly in the rising conflict

---

[26] John Selby, 'Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?' (2017) 25 International Journal of Law and Information Technology 213 <https://doi.org/10.1093/ijlit/eax010> accessed 15 May 2021.

[27] Article 29 Data Protection Working Party, 'Statement on Data protection and privacy aspects of crossborder access to electronic evidence' (2017) 4 28 Commission (n 25) 6

[28] Chander. A & Uyên P. Lê, 'Data Nationalism', 64 Emory L. J. (2015) at 680- ; Bagchi, Kaushambi; Kapilavai, Sashank, 'Political Economy of Data Nationalism', (22nd Biennial Conference of the International Telecommunications Society (ITS), June 2018)-'.

[29] sujithxavier, 'Digital Colonialism and the World Trade Organization' (TWAILR, 20 November 2019) <https://twailr.com/digital-colonialism-and-the-world-trade-organization/> accessed 14 December 2021.

[30] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981.

[31] For instance Austria utlises the GDPR as its baseline data protection statute and domesticated it in the form of the Austrian Data Protection Act (Datenschutzgesetz), Federal Law Gazette I No. 165/1999, para. 46

between governments and corporations, especially multinationals, people and personal rights are, in fact, the heart of the debate.[32]

While most scholars on the matter state that data nationalism is motivated by a collective nativist agenda of the state, in the EU, the statute and case law reflects that the struggle for data protection and privacy is a personal one.[33] The significant points of conflict in EU data protection law are ensuring that people know who is processing their data, who is accessing the data, what they are doing with the data and if the data is safe in the processors' custody.

Kamleitner and Mitchell have noted that the uniform set of rules created by the GDPR leads one to conclude that data protection legislation should only be made related to personal data under the GDPR.[34] This is principally because the GDPR only protects personal data.[35] The vast majority of applications of data nationalism as perfected by China relate to far more than personal data, such as important data, to protect the national security of the People's republic of China.[36]

The use of digital and electronic communication in our daily lives has risen tremendously in the past two decades. As a result of that profound rise, the attendant risks to national security and the digital safety and wellbeing of residents in the EU have also arisen in that period of time. Threats from the abuse of electric communication by non-state actors, hostile states, or even corporations with ill intentions are now serious concerns that governments must address.[37]

2.3. Data nationalism distinguished from data sovereignty

Data nationalism is usually associated with data sovereignty, and on occasion, the two terms are even used interchangeably. However, it is vital to highlight the distinction between the two terms in order to delve into the research on data nationalism properly. Data nationalism refers to measures that specifically encumber data transfers across municipal borders.[38]

---

[32] Rubistein, I. (2013), 'Big Data: The End of Privacy or a New Beginning?', International Data Privacy Law, Vol. 3, No. 2, pp. 74–87.

[33] W Kuan Hon, Data Localization Laws and Policy : The EU Data Protection International Transfers Restriction through a Cloud Computing Lens (Edward Elgar Publishing Limited 2017) <https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=1526350>.

[34] 'Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements - Bernadette Kamleitner, Vince Mitchell, 2019' <https://journals.sagepub.com/doi/10.1177/0743915619858924> accessed 13 December 2021.

[35]'EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1'. (General Data Protection Regulation (GDPR)) Article 4(1) <https://gdpr-info.eu/> accessed 27 August 2021.

[36]Zheng (n 15).

[37]Russell Hsiao, 'Implications for the Future of Global Data Security and Privacy: The Territorial Application of the Stored Communications Act and the Microsoft Case' (2015) 24 Catholic University Journal of Law and Technology 215 at 218 <https://heinonline.org/HOL/P?h=hein.journals/cconsp24&i=217> accessed 30 October 2021.

[38] Chander. A & Uyên P. Lê, 'Data Nationalism', 64 Emory L. J. (2015) at 680- ; Bagchi, Kaushambi; Kapilavai, Sashank, (n 17).

Oftentimes data nationalism is performed by implementing restrictive laws mandating the localisation of data. Thus, multinational companies must establish local data storage facilities in respect of all data sourced from that country.

On the other hand, data sovereignty is the concept that a country has complete control over the entirety of personal data stored, created, or collected in that country.[39] Data sovereignty as a concept has existed in different forms since writing became a tool. However, the concept as commonly known today is culled from the US PATRIOT Act.[40] The PATRIOT ACT is famous within the discussion of data protection for controversially inadvertently enabling US Law Enforcement officials to access any data physically found within a server in the United States regardless of where the information had originated.[41]

This theory of data supremacy was tested out by the Courts of the United States of America in the case *Microsoft Corp* v *the United States*[42] in 2018 after Microsoft challenged a warrant for access and surrender of emails of a target account in a drug trafficking investigation which was stored in Ireland which was made by the Federal Bureau of Investigation (FBI). Microsoft's argument was the warrant was issued under Section 2703 of the Stored Communications Act and thus applied solely to data stored within America.

Therefore, Microsoft believed that American companies could not be compelled to produce data stored in servers outside the United States of America. The case was never fully heard because, by the time the US government's appeal to the Supreme Court of the United States (SCOTUS) was heard, the United States legislature had passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[43] into law. The CLOUD Act gave American law enforcement agencies unrestricted access to all data stored by American companies through their remote cloud servers. This power was independent of the server being hosted outside the United States of America. Thus, when the case came to the SCOTUS, it was held that the argument was already moot.

From the above, it can be surmised that data sovereignty will apply irrespective of where the data is stored, unlike data nationalism which solely applies to the protection of the data of the residents by ensuring the data is stored locally. Furthermore, data sovereignty gives the sovereign state power to access, collect, process, and store the data of its residents.

Cory and Dascoli note that analysis of both concepts from a practical point of view (which is the point of view of most businesses that currently process data) immediately leads to the conclusion that both of these concepts amount to severe digital barriers to cross-border

[39]Andrew Keane Woods, 'Litigating Data Sovereignty' (2018) 128 Yale Law Journal 328 <https://heinonline.org/HOL/P?h=hein.journals/ylr128&i=356> accessed 3 September 2021.

[40] United Nations High Commissioner for Refugees, 'Refworld | United States of America: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act)' sections 210,212 and 215 (Refworld) <https://www.refworld.org/docid/3dea43144.html> accessed 30 October 2021.

[41] Hsiao (n 37).

[42]United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (201 Per Curiam, '17-2 United States v. Microsoft Corp. (04/17/2018)' 3.

[43] H.R.4943 - CLOUD Act115th Congress (2017-2018)

data transfers.[44] Thus, while both policies are distinct, they still inherently have a nativist ideal to protect the residents of the state and the state itself as their foundation. Hence, for the purposes of this thesis, they will be collectively identified as data nationalism policies.

2.3.1. Justifications and challenges for data nationality

Data nationality does not exist in a vacuum. The need for this type of policy results from several crucial socio-political factors. The two significant factors that justify its existence are:

a. The need for increased security, and
b. The monetary benefits.

According to Ellington, data nationalism as a concept has increased in popularity because of the increased need for security. Many Countries are quite critical about national security and the safety of their residents. Some may say that this criticality is often to the point of obsessive mistrust.[45] As a result, there is increased spending in surveillance and counter-surveillance[46] with the sole aim of protecting the state. The existence of big data raises both opportunity and risk for such states as the data can be analysed as a form of surveillance over the state's residents and adversaries.

However, there is also the risk that the state's adversaries will take custody of that data and analyse it to determine weaknesses which could also raise some severe complications. Thus, it only makes sense for such states to retain full and final power over all data created and utilised by residents in the incidence of data sovereignty. In the incidence of data nationalism, the need to protect the residents is spurred from the desire to ensure that the residents' data is secure. Within the broader context of legitimising international transfers of data, the European Union Court of Justice recently invalidated the primary legal treaty to transfer data between the US and the EU in *Schrems II.*[47]

Whilst from a technical perspective, data may be viewed as a virtual, intangible substance, the emerging legal reality is that even beyond specific privacy legislation, where data is sourced can in and of itself materially limit businesses' ability to share, utilise and monetise that data. Additionally, indigenous people have relied on data sovereignty policies to protect their group from extinction or erasure in recent years. An excellent example of this is the data sovereignty rights exercised by the Mauri indigenous people of New Zealand over any Mauri data recognised in New Zealand municipal law and international law.[48]

Data nationalism offers immense monetary benefits. The economic rationale for data nationalism policies is similar to countries' arguments for trade restrictions globally. Data nationalism and forced data localisation ensure that companies have a physical presence in the

---

[44] Nigel Cory and Luke Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them' [2021] INFORMATION TECHNOLOGY 90.

[45] Thomas C Ellington, 'Won't Get Fooled Again: The Paranoid Style in the National Security State' (2003) 38 Government and Oppositiona at 436 <http://www.jstor.org.tilburguniversity.idm.oclc.org/stable/44483044> accessed 31 October 2021.

[46] 'The Mataatua Declaration on Cultural and Intellectual Property Rights of Indigenous Peoples' 1993, Article 5.

[47] Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ('Schrems II') (2020) C-311 1 18

[48] The United Nations, Declaration on the Rights of Indigenous Peoples of the General Assembly, A/RES/61/295, Articles; 1,2,3,7,8,9,11,12,15,16,21, 25, 27, 31, 39.

state in question.[49] It could involve having domestic servers in that country or region dedicated solely to storing that company's data. It may also entail simply banning foreign companies and having local options solely, who is established in that country/ region, regulated by the laws of that country/ region, and having all the data those companies process stored in that country/ region.

This ringfencing technique is becoming more popular, especially since the big data and data analytics market is a highly profitable industry that earned an estimated USD 139 billion in 2020.[50] While data nationalism has its advantages for the government and data subjects, it also raises concerns for businesses because those businesses resident in data nationalism regimes will be unable to take advantage of the opportunities afforded by more affordable storage options around the world. A fairly typical example is that data nationalism policies make data sharding extremely difficult in practice.[51] Cattell defines data sharding as when a piece of data is split into several smaller units, also known as 'shards'. The shards are then cached into multiple data centres to minimise costs and improve the controllers' data redundancy mechanisms significantly.[52]

Additionally, the diverse identity of data nationalism regimes and the forms those legislations take has raised immense regulatory and compliance concerns for multinationals, which have resulted in increased overhead expenses, especially in light of the various, conflicting legal regimes and requirements the companies are forced to balance. The risks are also multiplied with the sharp rise in data localisation legislation globally, as well as steep sanctions for data-related mishaps. These legislations will be mentioned, and the European and Chinese legislation will be analysed in the following chapter.

2.4. Different forms of data nationalism

Many scholars have discussed the various components of data nationalism laws. Hill addressed this issue and stated that data nationalism usually takes the shape of any statute or regulation that can encumber the movement of data across national borders or limit where and by whom they are stored or processed.[53] As a result, they can be a combination of measures used simultaneously.

---

[49] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')'EUR-Lex - 32000L0031 - EN' (Official Journal L 178 , 17/07/2000 P. 0001 - 0016;) <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN> accessed 31 October 2021.

[50] Markets & Markets, 'Big Data Market by Component, Deployment Mode, Organization Size, Business Function (Operations, Finance, and Marketing and Sales), Industry Vertical (BFSI, Manufacturing, and Healthcare and Life Sciences), and Region - Global Forecast to 2025', (2020), TC 1521

[51] Richard D Taylor, 'Data Localization': The Internet in the Balance' (2020) 44 Telecommunications Policy 102003 <https://www.sciencedirect.com/science/article/pii/S0308596120300951> accessed 31 October 2021.

[52] Cattell, Rick, 'Scalable SQL and NoSQL Data Stores' (2011) 39 Sigmod Rec. 0163-5808 https://doi.org/10.1145/1978915.1978919

[53] J Hill, 'A Balkanized Internet? The Uncertain Future of Global Internet Standards' (2012) Georgetown Journal of International Affairs 49-58, at 49.

Data nationalism legislation can come in the form of blanket embargos on information leaving a particular territory.[54] This means that the state, through legislation, limits the transfer of information out of the country. For the purpose of this thesis, this technique will be referred to as hard data nationalism. The most prominent proponent of hard data nationalism is the People's Republic of China (PRC).[55] Through Article 37 of the Cybersecurity Law of the People's Republic of China (CSL), the PRC mandates that all critical information infrastructure operators ('CIIOs') must store all the personal information and essential data generated from the critical infrastructure of information within mainland China.[56] India is also test running hard data nationalism through its Data Protection Bill of 2019.[57]

The advantage of a hard data nationalism policy is that it generally aids in building local capacity to innovate. For instance, China and India have experienced leaps and bounds in technological innovation since adopting data nationalism and local content targeted legislation.[58] The major disadvantage, especially for a state that is not centrally planned but desires to implement hard data nationalism, is that it restricts freedom of choice and trade. Hard data nationalism, in essence, turns the state utilising it into a digital island. If the state does not have local capacity at the time of passing the legislation, it will struggle to compete technologically. Trade restriction litigation is also possible if a World Trade Organisation member country undertakes hard data nationalism.[59]

Mishra has pointed out that data nationalism can also be in the form of some regulations mandating information to be stored domestically.[60] This simply means that all data processed in a state must be resident in that state. In order words, the data is *localised*. The European Union law regulates the processing of personal data within the EU through its detailed and rights centred data protection law called the GDPR (General Data Protection Regulation). The GDPR requires that all data collected on EU residents be either stored in the EU to make them subject to European data protection laws or within a jurisdiction with similar levels of protection.[61]

Additionally, this provision is applicable to both data controllers and data processors to capture all parties who have access to personal data fully. It must be noted that the personal data of European residents need not necessarily be stored in solely the EU under the GDPR. However, the requirements for storing that data outside the EU may sometimes be deemed too restrictive to sufficiently reduce the concerns of data localisation.

---

[54] N Mishra, 'Data localization laws in a digital world: Data protection or data protectionism?' (2016) Public Sphere Journal 135-158, at 139, available at https://psj.lse.ac.uk/articles/45/galley/44/download/ (accessed May 14, 2021)

[55] 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)' Article 37(New America) <http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/> accessed 16 August 2021.

[56] Cyber Security Law of the People's Republic of China (2017)

[57] Anirudh Burman Sharma Upasana, 'How Would Data Localization Benefit India?' (Carnegie India) <https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291> accessed 31 October 2021.

[58] ibid.

[59] Selby (n 26).

[60] Mishra, note 7 above, at 139; Chander and **L6,** note 1 above, at 680; Ahmed and Chander, note 2 above, at 6.

[61] General Data Protection Regulation, Art. 45.

Furthermore, some countries have imposed specific restrictions amounting to forced data nationalism, such as rigid controls on data transfers in particular sectors such as finance or health.[62] The EU explicitly mandates restrictions in data transfers through the GDPR. The Data Security Law imposes strict data localisation requirements in the PRC.[63] This, in turn, raises concerns about cross-border trade.[64]

Additionally, data nationalism can occur through exercising jurisdiction over controllers or processors that are not located within the state processes data of data subjects that reside in the state. This is often called the extra-territorial jurisdiction of the GDPR, and it is the EU's innovation on data nationalism. It ensures that EU data subjects are always protected wherever in the world they might be and ensures that controllers and processors that target EU data subjects must meet the requirements of the GDPR or face being penalised.[65]

Multinational businesses with a physical presence in the EU increasingly find themselves trapped in a dilemma getting data out of the EU. Those data transfers are hinged on the importance of big data analytics in product management.[66] The enactment of the GDPR and all the additional regulations and case law on the expanding scope of data and data transfers have only made data transfers more complicated. Thus, multinational businesses with a physical presence in the EU are confronted with seemingly constricting legal obligations in accordance with EU law.

Restrictions in transfers pose some severe concerns because, by definition, a data transfer implies that the data created in the EU or belongs to an EU resident was moved to a data centre outside the EU to be processed. Additionally, it also implies that an employee of a multinational with a presence in the EU accesses data created within the EU while being outside the EU. This is very likely to happen with the global tech economy, where data analysts and developers work remotely for a multinational in various parts of the world.[67] Thus, as a result of all the above-mentioned forms of data processing being termed as data transfers, conflicts arise on how exactly one should process European Data so as not to run afoul of the GDPR.

One of the consequences was the setting up of European offices, data centres and divisions in many multinationals to process the data locally. However, that is not without costs as it raises concerns on how the different country offices of a multinational will be able to relate with each other and the data of each other. Thus, many multinationals now store and process

---

[62] Erica Fraser, 'Data Localisation and the Balkanisation of the Internet' (2016) 13 SCRIPTed 359 <https://script-ed.org/?p=3185> accessed 15 May 2021.

[63] Data Security Law of the Peoples Republic of China (2021) Article 36 '中华人民共和国数据安全法' (China Law Translate, 10 June 2021) <https://www.chinalawtranslate.com/datasecuritylaw/> accessed 31 October 2021.

[64] Zheng (n 18).

[65] Brendan van Alsenoy (2017), Reconciling the (extra)territorial reach of the GDPR with public international law in Gert Vermeulen and Eva Lievens (Eds), Data Protection and Privacy under Pressure Transatlantic tensions, EU surveillance, and big data, pp. 77-100, available at https://lirias.kuleuven.be/retrieve/481782

[66]The United Nations Conference on Trade and Development Secretariat, 'The Value and Role of Data in Electronic Commerce and the Digital Economy and Its Implications for Inclusive Trade and Development' (2019) Trade and Development Board Intergovernmental Group of Experts on E-commerce and the Digital Economy Third session Geneva, at 18.

[67] Alex Capri, 'Techno-Nationalism: What Is It And How Will It Change Global Commerce?' 7.

their data in multiple countries and keep a Chinese wall between the various offices' data to properly navigate the legal and regulatory terrain. It must be noted that transfers are acceptable if they follow the GDPR's data protection principles or, in the alternative, utilise a unique data residency-as-a-service provider to aid in protecting the data during transfers.[68]

Flowing from the above, the relationship between the US and the EU is extremely crucial in addressing these concerns from a European perspective. This is mainly due to the massive influx in cross-border trade between the EU. The US raises further credence to the fact that the amount of data shared between the two power blocks is so voluminous that it is almost indistinguishable quite difficult to sort. Furthermore, in the investigation of cross border crimes or regulatory concerns, the US law enforcement agencies often seek access to data processed by a provider based in Europe.[69] This is necessary because many US providers have subsidiaries that operate data centres, in which personal data of relevant for US criminal and regulatory proceedings may be stored.[70]

Thus, the seamless transfer of data between the US and the EU is essential and fundamental to the trade relations between these two intertwined power blocks. However, the GDPR did not specifically mention transfers could be done with the US, thus raising concerns on how best data transfers can be effected between the two blocks. The EU and the US utilised a safe harbour agreement in order to facilitate data transfers without running afoul of the EU data regime. In the advent of the Court of Appeals decision in the aforementioned case of *Microsoft* v *The United States,*[71] the CLOUD Act was passed into law in order to forestall the calamity that potential defeat in the Supreme Court would have caused. The CLOUD Act gave American law enforcement powers to access data stored in servers outside the United States.[72] This legislation was against every principle that the European Privacy laws and data protection and data privacy laws stood for.[73]

As a result of the American Law Enforcement Agencies intrusive interference into privacy that was brought to light by Edward Snowden, an Austrian privacy advocate named Maximilian Schrems filed a complaint against Facebook on the transfer of his data from Ireland to the US. In the complaint, Mr Schrems challenged the transfer of his data (and the data of all EU residents' generally) to the United States by the Facebook European Office, which is incorporated in Ireland. That case, commonly known *as Schrems I,*[74] led the Court of Justice of the European Union on October 6, 2015, to invalidate the Safe Harbour arrangement, which had previously governed data transfers between the EU and the US. The result of the decision in *Schrems I* and the consequent invalidation of the previous Safe Harbour arrangement

[68] Chapter V of the GDPR covers transfers in depth

[69] Refugees (n 40).

[70] Letter from Peter J. Kadzik, Assistant Attorney General, to Joseph R. Biden, President of the U.S. Senate (15 July 2016) 2

[71] Curiam (n 42).

[72] CLOUD Act,

[73]'CLOUD Act Agreements from an EU Perspective | Elsevier Enhanced Reader' <https://reader.elsevier.com/reader/sd/pii/S0267364920300479?token=CB96C61EB206345F1F6A42FAB3A220769D972A721F32C29F6C6D96A4BD1C5DADD27E02965FB72F640D60880A3C7E9EAA&originRegion=eu-west-1&originCreation=20211213020959> at 2 accessed 13 December 2021.

[74] Schrems -v- Data Protection Commissioner [2014] IEHC 310 (IEHC (2014)).

between America and the EU made it necessary to create a 'privacy shield' between the US and the EU to permit the transfer of data.[75]

Following the creation of the 'privacy shield', Mr Schrems filed another complaint on the legality of the privacy shield, and the CJEU agreed with his submissions again. Thus, the 'privacy shield' was not a long-term solution as *Scherms II* struck it down. The invalidation of the EU- US Privacy Shield by the Court of Justice of the European Union (CJEU) in *Schrems II*[76] implies that personal data in the EU is not to be transferred except within the parameters of the GDPR. The case signifies that the EU will defend the right to data of its residents at all costs.

When one considers that these policies were enacted to protect EU residents or the national security of EU states and juxtaposes this fact with the need for a free and open Internet and global access to information, the need for a detailed analysis of the conflict, and the need for possible solutions seem compelling. Proponents of data nationalism believe that a state's big data are of strategic economic, political and military interest and, thus, should not be used freely by non-state actors.[77] However, do those concerns pale in contrast to the practicality of turning a vibrant state with cross-border transfers into a digital island?

It is of utmost importance that any such solutions raised, the protection of the fundamental right to data protection under the European legal framework, does not get undermined. Hence, this thesis will play a pioneering role in exploring and proposing the necessary safeguards that must be included in applying and creating data nationalism policies to prevent the further Balkanisation of the Internet.

The different forms of data nationalism aid in thoroughly understanding the concept and identifying data nationalism anytime a state adopts a policy. The diverse conditions ranging from hard data nationalism to a more flexible format will decide how countries will interact over data transfer and data storage. The various methods usually adopted for data nationalism are likely to create a plethora of outcomes, one of which is the additional Balkanisation of the Internet and municipal tech policies that may be increasingly nativist to mitigate the fallout that will arise from existing global distrust. [78]

2.5. Conclusion

The appeal of data nationalism is not rooted within the context of actively trying to restrict trade but as a result of the desire to ensure that due process is carried out with the data of the data subjects at all times. For most governments today, data is indeed the new oil, and as such, it ought to be protected jealously. For some others, the need to access data should not

---

[75] Publications Office of the European Union, 'C/2016/4176, Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield (Notified under Document C(2016) 4176) (Text with EEA Relevance)' (12 July 2016) <http://op.europa.eu/en/publication-detail/-/publication/c183d956-57a6-11e6-89bd-01aa75ed71a1/language-en> accessed 27 August 2021.

[76] Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ('Schrems II') (2020) C-311 1 18

[77] Chander. A & Uyên P. Lê, 'Data Nationalism', 64 Emory L. J. (2015) at 680- ; Bagchi, Kaushambi; Kapilavai, Sashank, 'Political Economy of Data Nationalism', (22nd Biennial Conference of the International Telecommunications Society (ITS), June 2018)-

[78] Fraser (n 62).

be restricted to a country's borders. Within those two schools of thought, there is a need to strike a fair and reasonable balance. The legal regime for data nationalism is intricate, with several rules differing in various states. The legal regime within the context of the EU and China will be scrutinised thoroughly in the following chapter within the context of the fears of the Balkanisation of the Internet.

Chapter III – The Legal Framework Governing Data Nationalism

3.1. Introduction

The legal framework governing most European and Chinese laws that may include data nationalism has helped clarify the positions of the EU and the PRC. Those laws have also raised considerable doubts about interconnectivity. This chapter will delve into the extent to which personal data may be protected under the EU and PRC may be under nationalism policies. To that end, the current legal framework within which data nationalism works in the EU and the Chinese legal framework on the localisation, storage, and transfer of data will be evaluated.

This chapter will then go into detail to analyse the scope of the applicable legal provisions such as the GDPR) and EU member state laws and all the recent policy considerations raised by the GDPR. Additionally, this chapter will also consider the Personal Information Protection Law, Data Security Law and the Cyber Security Law of the People's Republic of China with an emphasis on the Chinese position on data nationalism.

3.2. Data Nationalism in the EU

The previous chapters have explained the concept of data nationalism in great detail; thus, there will be no need to define the concept again generally. However, within the context of the EU, there is a need to scrutinise the available EU laws naturally and within the EU Member States to understand the data nationalism policies of the EU. It must be noted that neither the EU nor its Member States possesses hard data nationalism legislations that mandate data localisation or fully restrict transfers like the People's Republic of China.

A rudimentary reading of the GDPR and ePrivacy Directive and various local Data protection laws of EU states indicates that neither the EU nor its Member States imposes strict data localisation requirements. Additionally, the statute that preceded the GDPR, the Data Protection Directive (95/46/EC),[79] is absent from direct data localisation or data residency requirements. The Directive and the GDPR establish methods for transferring data outside the EU, thereby ensuring that data transfers are permissible under the aforementioned legislation.[80] There are specific requirements for localisation of data within EU states for political data.

The Netherlands, for instance, in The Public Records Act 1995 requires all Dutch administrative authorities to store certain types of data in repositories located within The Netherlands (Section 1(f)). Section 26 establishes a central state repository in The Hague for public records of central government bodies and state repositories in the capital of each province for public records of state bodies established in that province.[81]

In the issue of data nationalism analysis, it is crucial to understand that data resident in one country that is accessed by employees of a company in a separate country counts as a data

---

[79] United Nations High Commissioner for Refugees, 'European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995, Available at: Https://Www.Refworld.Org/Docid/3ddcc1c74.Html'(Refworld)<https://www.refworld.org/docid/3ddcc1c74.html> accessed 13 December 2021.

[80] Chapter V of the GDPR deals exculsively with Data transfers

[81] Act of 28 April 1995 replacing the Public Records Act 1962 (Bulletin of Acts and Decrees, no. 313) 'Machine Translation of 'Public Records Act 1995' (Netherlands)' <https://www.global-regulation.com/translation/netherlands/3074258/public-records-act-1995.html> accessed 13 December 2021.

transfer.[82] For instance, if data is stored in the Netherlands and the company has a team of engineers located in Nigeria, anytime that team accesses the data for customer support services in Nigeria counts as a data transfer. The above scenario counts as a data transfer because the data has technically been moved out of the Netherlands, where it is resident, to Nigeria, where the customer support team is resident.

Additionally, as a result of recent fintech innovations, payment processing functions often occur within multiple countries as the issuing bank, the acquiring bank, the payment gateway and the settling bank may sometimes be located in separate countries. This results in a data transfer each step of the way.

These data transfer rules have been in existence in the European Union since the 1995 Data Protection Directive (DPD).[83] The sharp rise in the interconnected digital economy and the increased use of digital outsourcing and a global remote working environment have led to a steady increase in reference to the provisions on transfers in recent years. The issue has been raised legally and scrutinised in detail after the landmark decision of the CJEU in *Schrems.*[84] In *Schrems,* the Court made clear that transfers of personal data to a third country, even if that transfer is from the servers of the same entity to its office in that third country, constitutes processing of personal data.[85] That entity in a third country is obligated to comply with the Data Protection Directives provisions on data processing and supervision. The Court, in addition, held that the high level of protection of personal data must be ensured during data transfers to a third country,[86] in accordance with Article 8(1) Charter of Fundamental Rights of the European Union (CFR).[87] As a consequence of the decision in *Schrems,* every transfer of personal data must fulfil a two-step test to be lawful: The first step is that the transfer must be based on one of the legal grounds for data processing. [88] The second step is that all transfers must conform to the conditions provided in Chapter V of the GDPR.[89]

It is indeed confounding that there is no generally accepted definition of the term 'data transfer' in existence within the data protection laws around the world despite how crucial the need for conditions on transfers are. Additionally, there is no definition of the term included in Article 4 of the GDPR.[90] The legal confusion caused by the current lack of a unified

---

[82] W Kuan Hon, Data Localization Laws and Policy : The EU Data Protection International Transfers Restriction through a Cloud Computing Lens (Edward Elgar Publishing Limited 2017) at 2<https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=1526350>.

[83] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 124 Schrems (n 20) para 45

[84] C-362/14, Maximilian Schrems v. Data Protection Commissioner [GC], 6 October 2015

[85] Schrems (n 20) para 45

[86] Schrems (n 20) para 72

[87] Charter of Fundamental Rights of the European Union [2012] OJ C326/391

[88] European Data Protection Board, 'Guidelines on derogations of Article 49 under Regulation 2016/679' (2018) 2/2018, 3; Paul Voigt, Axel von dem Bussche the EU General Data Protection Regulation – A practical guide (2017) 117 128 Recital 101 GDPR

[89] ibid

[90] Liane Colonna, 'Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbour Program?' (2014) 4 International Data Privacy Law 217

definition of 'data transfers' has been repeatedly criticised by the European Data Protection Supervisor (EDPS).[91] The rise of Web3, cloud technology, decentralised ledgers and the ever-increasing interconnectedness between global business entities have raised strong arguments among some legal scholars, think tanks and policy analysts for the abandoning of the current concept of data transfers and the establishment of uniformed international rules and procedure for international data processing.[92]

The extraterritorial jurisdiction of the GDPR in Article 3(2) is a key feature of the GDPR utilised in exercising jurisdiction over data transfers that the GDPR should ordinarily not be privy to. While the GDPR's reference of 'cross-border' transfers in Article 3 (2) seems to imply the involvement of more than one country in the transfer, in reality, that is not the case. The GDPR only refers to the final destination of the data when 'cross-border' transfers of data are mentioned. That final destination must always be a controller or processor in a third country or an international organisation. What occurs in practice is that under the GDPR, all the controllers or processors that are subject to regulation under the GDPR must comply with all the provisions of data transfers to third countries, as highlighted in Chapter V of the GDPR.

In *Weltimmo v Nemzeti* [93] the Court of Justice addressed the issue of an establishment to include the targeting of EU data subjects even though one does not have a strong physical presence in the Union. In addition, although the United Kingdom is no longer a member of the EU after BREXIT, the High Court of England and Wales in *Soriano v Forensic News LLC and Others*[94] considered that where there was no establishment nor specific targeting of EU data subjects a foreign entity, in the instant case, an American website could not be construed to be under the jurisdiction of the GDPR.[95]

3.2.1. Transfers or disclosures not authorised by Union law

The majority of the provisions in Chapter V of the GDPR are based on identical provisions in the former Data Protection Directive. One of the innovations of the GDPR is Article 48, which has no counterpart in the former Directive.[96] Article 48 essentially reproduces the general position of the law hitherto that transfers of personal data to a third country may only be made pursuant to a judgment or decision of the judicial or administrative authority of the third country were based on an international agreement, such as a Mutual Legal Assistance Treaty (MLAT). [97] Article 29 Data Protection Working Party echoes this preference for transfers of personal data through an MLAT.[98] A noticeable distinction is that the Working

[91] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the potential of Cloud Computing in Europe'' (2012) 17

[92] Paul M. Schwartz, 'Information Privacy in the Cloud' (2013) 161 University of Pennsylvania Law Review 1628, 1629

[93] Weltimmo v Nemzeti Adatvédelmi és Információszabadság Hatóság [2015] Court of Justice of the EU, Judgment (C-230/14,), ECLI:EU:C:2015:639 ECLI :639.

[94] Soriano v Forensic News LLC & Ors [2021] EWHC 56 (QB) (EWHC (QB)).

[95] ibid. At 45-60

[96] European Data Protection Board (n 127) 4

[97] Albrecht (n 8) 6

[98] Article 29 Data Protection Working Party, 'Opinion 05/2012 on Cloud Computing' WP 196 23 168 Recital 115 GDPR

Party's recommendation demands the enforced use of MLATs, while GDPR only cites MLATs as an illustration of such an international agreement. This ensures that transfers may also be based on other forms of international agreements other than MLATs.

The EU and its member states may, nonetheless, possess data protection legislation that permits the European data protection authorities to exert significant control over data retention and thereby enable the European data authorities to acquire greater control over compliance. Additionally, the EU encourages its data controllers to store and process data within the EU or within certain countries that are deemed to possess an equivalent level of data protection measures as in the EU.

Countries that do not meet that threshold are not considered as 'adequate' data protection regimes and thus are restricted from accessing or processing EU data generally.[99] The adequacy decisions and the fact that employees in a different country accessing data count as a data transfer raises significant questions on the necessary steps to take to legally transfer data to a country that cannot protect data within the EU's guidelines adequately. The GDPR in Article 49 provides conditions that enable the constitution of a legal transfer of data outside of the European Economic Area (EEA) into a jurisdiction that possesses what may be termed 'inappropriate safeguards'. The various ways a legal transfer can be effected consist of:

An adequacy decision can effect a legal transfer.[100] Adequacy decisions are an EU Commission decision that certifies that a country has data protection laws that offer either an adequate or commensurate protection level to the EU. At the moment, the EU has issued adequacy decisions in only fourteen (14) countries. These countries are Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, the United Kingdom under the GDPR and the LED, Uruguay,[101] and recently South Korea.[102]

Transfers can also be effected through binding Corporate Rules. This ensures that all the internal rules of a company that are binding are to be approved by data protection authorities.[103] There is an additional option for standard contractual clauses/ model clauses in order to effect transfers. These are individually negotiated contracts that are made between the controller and processor.[104] While its relevance may be questioned, the privacy shield was an additional method of effecting transfers. It existed for US companies only to replace the self-certification program for the Safe Harbour provision. Remarkably, it was struck down by the

---

[99] GDPR ibid. Article 45

[100] 'EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1'. Article 45 (General Data Protection Regulation (GDPR)) <https://gdpr-info.eu/> accessed 27 August 2021.

[101] 'Adequacy Decisions' (European Commission - European Commission) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 13 December 2021.

[102] 'EDPB Adopts Opinion on Draft South Korea Adequacy Decision | European Data Protection Board' <https://edpb.europa.eu/news/news/2021/edpb-adopts-opinion-draft-south-korea-adequacy-decision_en> accessed 13 December 2021.

[103] ibid Art. 46.

[104] 'Adequacy Decisions' (n 101).

Grand Chamber of the European Court of Justice in *Schrems II*,[105] like the safe harbour provision. American entities can now only rely on standard contractual clauses to transfer data.

3.2.2. Derogations for specific situations

Despite its general restrictions of data transfers to third countries in Article 48, Article 49 includes several necessary derogations for specific situations. Those derogations would help enable such transfers. The derogations in Article 49 make certation that third country data transfers are permissible regardless of whether the appropriate safeguards or adequate level of data protection are already put in place or not. Transfers in such situations are only meant to be conducted occasionally and on a needs basis. They are an exception made possible because of the extraordinary need to process the data and not a regular part of the course of actions available.[106]

As a result of the fact that the exception is only created for extraordinary processing and not day-to-day processing, large providers that receive a significant amount of data requests regularly cannot rely on this provision. This is simply because those large providers cannot guarantee that such data will only be transferred occasionally. According to Article 44, the application of all provisions in Chapter V, including Article 49, should never lead to a situation where the data subject's fundamental rights might get breached.[107] The major question to be raised by the above is whether the exception is adequate to manage the burgeoning need for processing worldwide. Additionally, the exception raises issues on how cloud-based multinationals may struggle to transfer data properly.

3.3. Data nationalism in the People's Republic of China

The People's Republic of China has taken a greatly different position from the EU to data nationalism. China has, over time, embraced data nationalism policies with strong requirements for data localisation and cross-border data transfer restrictions scattered in its laws. Previously those restrictions and requirements were not in one coherent statute but littered within the Cybersecurity Law of the People's Republic of China and sector-specific implementing regulations that follow the Cybersecurity law. [108]

The PRC's data nationalism legislation is additionally contained in various sector-specific regulations. The majority of those legislations possess specific requirements for data processing by entities in the specific delineated sectors.[109] For instance, Article 48 of the Law of the People's Republic of China on Guarding State Secrets (2010 Revision) restricts the transfer of any data related to the state secrets of the PRC outside mainland China. Other examples include, Article 24 of the Regulation on the Administration of Credit Investigation Industry, Article 6 of the Notice by the People's Bank of China Regarding the Effective

---

[105] Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, Case C-311/18

[106] European Data Protection Board (n 127) 5

[107] ibid 3

[108] Cybersecurity Law of the Peoples Republic of China (2017) John Selby, 'Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?' (2017) 25 International Journal of Law and Information Technology 213 <https://doi.org/10.1093/ijlit/eax010> accessed 15 May 2021.

[109] Zheng (n 15); Lili Zhang and others, 'A Review of Open Research Data Policies and Practices in China' (2021) 20 Data Science Journal 3 <http://datascience.codata.org/articles/10.5334/dsj-2021-003/> accessed 13 December 2021.

Protection of Personal Financial Information by Banking Institutions provides that personal financial information collected in the PRC must be stored, processed, or analysed in only in the PRC; with the exception of if it is permissible by another legislation or regulation to store process and analyse that data outside mainland China; Article 27 of the Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions and Article 27 of the Interim Measures for the Administration of Online Taxi Booking Business Operations and Service.[110]

With the passing of the Data Security Law and the Personal Information Protection Law, no general unified framework exists to guide the regulation of data transfers out of the PRC. This patchwork of requirements is expected to remain in practice even after the DSL and the Personal Information Protection Law (PIPL) are passed into law. The different restrictions relate to the status of the controllers and processors as well as the type of data that they intend to transfer outside the PRC.

3.3.1. Concepts of 'personal information' and 'important data'

There are two categories of data that might be subject to data nationalism policies through either localisation or cross border transfer restrictions under the CSL and the DSL. The two types of data subject to nationalism are 'personal information and 'important data'.

As indicated in the PIPL, personal information denotes the multiple types of electronic or otherwise recorded information that relates to natural persons that have either been identified or remain identifiable. It excludes anonymised data.[111] This definition of personal information is largely consistent with the definition in the concept stated in the CSL and other national standards such as the Information Security Technology - Personal Information Security Specification.[112]

Important data was introduced into Chinese jurisprudence in the CSL in its data localisation article[113] and was mentioned again in the DSL[114] within the context of the establishment of a categorised and graded protection system for data. It was, however, not mentioned in the PIPL. Rather, article 58 of the PIPL regulates what is termed a personal information handler that provides "important Internet platform services" with a large user base and what is categorised as a complex business model. Important data remains undefined under both laws. The PIPL additionally fails to tackle this concern.

The DSL, for instance, as opposed to clearly defining important data, requires the government to publish what is termed a national-level catalogue of 'important data'. Additionally, the DSL in Article 27 requests regional and sector-specific regulators to issue

---

[110] 'The Future of Data Localization and Cross-Border Transfer in China: A Unified Framework or a Patchwork of Requirements?' <https://iapp.org/news/a/the-future-of-data-localization-and-cross-border-transfer-in-china-a-unified-framework-or-a-patchwork-of-requirements/> accessed 31 October 2021.

[111] PIPL ibid, Article 3 Lothar Determann and others, 'China's Draft Personal Information Protection Law' (2021) 4 Journal of Data Protection & Privacy 235.

[112] People's Republic of China, Information Security Technology - Personal Information Security Specification, GB/T 35273-2020) (PI Specification)

[113] CSL ibid. Art 37

[114] DSL ibid. Art 21

more detailed catalogues to further identify the scope of what is classified as 'important data' within their regions and sectors.[115]

Hence, these catalogues, as a result, provide more guidance on a case-by-case level on all that data which should ordinarily fall within that scope. Within the context of the discussions on important data, it is important to note that even though the national level catalogue of what is termed 'important data is still pending, several regulators have implemented the collection and to that end have taken steps to define 'important data' within specific sectors.

The Cyberspace Administration of China's draft Measures on the Automotive Data Security Management[116] is a good example of how the sector can define what qualifies as 'important data'. The draft regulation provides a comprehensive list of what qualifies as 'important data' within the Chinese auto sector to include:

- Any data covering the flow of people and traffic in what is termed an important and sensitive area, such as places involving state secrets (for instance, military administrative zones or areas where national defence science and technology institutions are located) as well as places where government agencies at county level and above are located
- The surveying and mapping data which possesses a higher level of accuracy than what is provided in publicly available maps
- Any data detailing the organisation of electric vehicle charging networks
- Data relating to the type of vehicles and quantum of vehicular traffic on the road
- Audio and video data that records outside of a car, especially one that includes the personal data of other commuters and pedestrians, including the faces, voices, vehicular plate numbers etc
- Any other automotive data that is specified by CAC and other relevant departments of the State Council that might be deemed to impact national security and public interests[117]

Finally, the DSL has brought to fore the novel concept of 'national core data'. National core data is a subcategory of important data. It is defined as 'data related to (PRC's) national security, the lifeline of the national economy, people's livelihood and vital public interests' in Article 21 of the DSL.[118] However, because the ink on the DSL is barely dry, it is currently unclear whether national core data will be subject to specific data localisation or cross-border transfer requirements and restrictions. Chen and Son note that though from the definitions, it is expected that national core data will likely be treated with hard data nationalism regulations.[119]

---

[115] DSL ibid. Art 27

[116] 'Several Provisions on the Management of Automobile Data Security (for Trial Implementation)-Office of the Central Committee of the Communist Party of China' <http://www.cac.gov.cn/2021-08/20/c_1631049984897667.htm> accessed 13 December 2021.

[117] Ibid Art 3

[118] Jihong Chen and Jiabin Sun, 'Understanding the Chinese Data Security Law' (2021) 2 International Cybersecurity Law Review 209 <https://doi.org/10.1365/s43439-021-00038-3> accessed 4 January 2022.

[119]'Understanding the Chinese Data Security Law | SpringerLink' <https://link.springer.com/article/10.1365/s43439-021-00038-3> accessed 4 January 2022.

3.3.2. PRC's data localisation requirements

Only companies are termed 'critical information infrastructure operators' that are subject to data localisation requirements in China under the CSL.[120] The first factor usually considered before determining whether a company is subject to China's data localisation requirements is the classification of the company. The company needs to be adjudged as a critical information infrastructure (CII) operator to fall under the PRC's data nationalism regime.[121]

Critical information infrastructure operators are broadly defined to mean all infrastructure could endanger national or public interests if damaged under the CSL.[122] Examples of CII operators include companies in financial services, transportation, telecommunications, energy, water, public services, electronic government affairs and electricity. Chen and Son note that this definition is open to more interpretations as there is no finite assessment, list or gazette for what amounts to a CII operator.[123]

A detailed reading of the CSL, DSL and PIPL indicate a failure to clarify exactly how data localisation requirements correlate with cross-border transfer restrictions and requirements. This raises concerns about transfers and transfer requirements. Additionally, none of the pieces of legislation explains whether 'localisation' solely refers to the storage of data locally or localisation extends, ensuring other processing activities are done locally. Thus, it remains quite uncertain these obligations could influence corporate entities in practice. [124]

CII operators are required to store both personal information and 'important data' collected and generated in China locally under the DSL and CSL.[125] Although CII operators are subject to data localisation requirements, transfers of personal information and 'important data' for business are possible if the CII operator passes a security assessment.[126] The requirement for localisation under the PIPL for non-CII operators that are personal information processing entities (The Data controller equivalent in Chinese jurisprudence) is if the personal information processing entities process data 'in a volume that reaches the threshold specified by CAC'.[127] Personal information collected and generated must be stored within China in such situations.[128] Thus, there is no general data localisation requirement for non-CII operators. The threshold for what quantum exactly amounts to be liable for localisation remains unspecified.

It remains uncertain whether the localisation restrictions and requirements under the sector-specific regulations converge with the existing framework of both CII and non-CII operators in mainland China. For example, the draft Automotive Measures require all the operators in the auto industry to store 'automotive personal data' and 'important data' in mainland China. The Measures define 'Automotive personal data' to include personal information of the drivers, passengers and owners of the automobiles', and any information that

[120] ibid.

[121] Zhang and others (n 109).

[122] 'Understanding the Chinese Data Security Law | SpringerLink' (n 119).

[123] ibid.

[124] Zhang and others (n 109); 'Understanding the Chinese Data Security Law | SpringerLink' (n 119).

[125] Art 23 CSL and Art 21 DSL; 'Understanding the Chinese Data Security Law | SpringerLink' (n 119).

[126] ibid

[127] CSL Art 37 Chen and Sun (n 118).

[128] ibid

could be used to accurately describe behaviour and properly identify individuals.[129] The draft Automotive Measures do not specify whether the regulations apply to only CII operators. As a result, non-CII operators in the automotive sector might also need to store 'automotive personal data' and 'important data' collected by them that relate to automobiles within mainland China.

3.3.3. Cross-border data transfer requirements in the PRC

The DSL provides a lifeline for transferring personal information and 'important data' out of mainland China if the transfer is necessary for a business's corporate needs, and the business passes a CAC approved security assessment and other relevant government agencies.[130] This acts as an exception to the compliance of data localisation requirements CII operators. The requirements of the security assessment process remain unreleased.

Furthermore, separate consent must be obtained from individuals by personal information processing entities (including both CII and non-CII operators) before their personal information can be transferred out of mainland China. This depends on whether consent is the lawful basis for processing. Additionally, the personal information processing entities ought to carry out internal risk assessments prior to transfers. This is similar to the requirement to provide a data protection impact assessment under the GDPR and the subsequent obligation to keep records of the assessment processing activities.

Additionally, the PIPL imposes different additional requirements for two classes of operators, which is assessed based on the volume of data the operator may plan to transfer.[131] Non-CII operators that process what is termed 'large volumes' of personal information are mandated to undergo a CAC administered security assessment.[132] As previously noted in other regulations of the PIPL, there has been neither mention of the necessary specific process the security assessment will take, nor mention of the quantum of the threshold.

Non-CII operators that fail to the threshold in the PIPL need to identify and utilise any one of the following lawful transfer mechanisms in order to lawfully transfer data out of mainland China:

- Obtain a personal information protection certification that can be issued by professional institutions in accordance with rules specified by the CAC
- Entering into an agreement based on a standard contract as stipulated by CAC with the recipient (the format of the standard contract has not yet been published)
- Other conditions that may be stipulated by laws and regulations which are not mentioned[133]

3.4. Reconciling the provisions

The EU and Chinese positions on data nationalism are quite different in approach and in implementation. The European position is in furtherance of the EU's desire to protect the rights of its residents.[134] As such, the restrictions in transfers out of the EEA, while a little

[129] Art

[130] Art 31 DSL;Chen and Sun (n 118).

[131] ibid

[132] ibid

[133] ibid

[134] The Recital of the GDPR points to the fact that it is a Human Rights centered legislation

stringent, are still quite *laissez-faire* with allowances for transfers if there is valid consent from the data subject every step of the way.[135] The odd localisation policy exists within individual legislation for the EU Member States, but it usually relates to really sensitive data such as health data or the data of government institutions and law enforcement.

On the other hand, the PRC's position is taken to protect the collective interests of the PRC and its Citizens, and the legislations execute that intention appropriately. An example is in the localisation of banking data and data related to taxies and livery businesses in China. Furthermore, the PRC's position is filled with reciprocity for states termed Hostile.[136] The consequence of localising and restricting transfers to that data is that it will be impossible for a non-Chinese entity to attempt to enter these markets or even predict the growth of the markets because there will be no big data to analyse and come to a business conclusion.

3.5. Conclusion

This chapter has highlighted that the GDPR, PIPL, the DSL and the CSL all exhibit some form of data nationalism policies. The GDPR remains silent on the localisation of data, but data localisation occurs in the EEA through legislation of EU Member States. The GDPR regulates and restricts transfers through Chapter V, but as noted, it gives allowances for transfers through special parameters that ought to be met. The GDPR exercises its data nationalism through extraterritorial jurisdiction, thus ensuring companies that target EU data subjects remain under the jurisdiction of the EU even if the data is being processed or accessed in a third country with no presence in the EU.

As a result, failure to comply comes at the risk of punitive punishment by virtue of a hefty administrative fine of up to twenty million Euro or 4% of their total worldwide annual turnover, depending on which is higher, in situations where personal data is transferred to a third country in contravention to the guidelines and set out standards in the GDPR.[137] This, thus, sometimes puts multinational business entities with subsidiaries in the EU between a rock and a hard place when it comes to transfers. On the other hand, the Chinese have taken a stricter approach to data nationalism.

The DSL and the CSL possess articles that mandate the localisation of data as well as restrictions in the transfer of data. Several sector-specific legislation in different areas of the Chinese economy that are deemed important also possesses strict data nationalism and localisation requirements. These legislations were made to protect the PRC. The passing of data nationalism laws raises issues on enforcement. De Hert has indicted with certainty that enforcement of the restrictions to transfers can be exercised by using existing instruments of international law.[138] Svantesson, on the other hand, is concerned that the GDPR' and other pieces of data protection legislation might be trying to regulate more than is deemed possible.[139]

---

[135] Article 4 GDPR

[136] Determann and others (n 111).

[137] Article 83(5) GDPR

[138] Paul de Hert, Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider

[139] Dan Jerker B. Svantesson, 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation' (2015) 5 International Data Privacy Law 232 184

However, it is important for the GDPR to be enforceable in these situations because failure to do so may undermine the effectiveness and then the legitimacy of the GDPR outside the European Economic Area (EEA).[140] In any case, further clarification by the legislator or the European Data Protection Board (EDPB)[141] on what exactly constitutes a 'data transfer to a third country' seems quite necessary in order to provide legal certainty for companies and EU data subjects alike. The PCR, through its strong state apparatus, can guarantee compliance with its data nationalism policies. There is a need for greater clarity on the meaning of several crucial terms that are used repeatedly throughout the various legislations, as well as a proper transparent interpretation of the volumes and thresholds that entail large processing.

[140] ibid 233

[141] Article 70(e) GDPR

Chapter IV-A Global data protection agreement as a possible way forward

4.1. Introduction

The previous chapters explicated concerns raised by the Balkanisation of the Internet. They further addressed the conflict presented by adopting data nationalism policies and the extent to which the EU and the PRC adopt data nationalism policies legally. This chapter will assess how data nationalism policies affect the concerns on the Balkanisation of the Internet. It will also identify legal and policy options to address this conflict and the feasibility of such solutions.

To this end, this chapter will analyse recent international developments and legal and regulatory techniques to contend with and combat data nationalism. The chapter will explore to what extent these approaches exacerbate the Balkanisation of the Internet and what end steps can be taken to resolve the established conflict.

4.2. Data nationalism and the Balkanisation of the Internet

Vinton Cerf and Bob Kahn created the Internet to be 'open, interoperable and unified'.[142] It was designed with no considerations for the national borders of any country or geopolitical or economic blocks. The Internet is facilitated by routing data across its network autonomously and automatically via the most efficient paths.[143] Internet data moves from location to location swiftly and in a seemingly arbitrary and unpredictable manner. This massive data movement is generally done without the user's knowledge or consent.[144] Fraser believes that the free flow of data across borders has enabled what can only be identified as unprecedented technical efficiencies and economies of scale in the storage and processing of data.[145] This has, as a result, revolutionised commerce and the ease and cost of doing business.

Data nationalism legislations are an antithesis to every critical feature of the Internet. Data nationalism legislations disrupt the free flow of data. Every new localisation requirement and transfer restriction will lead to further splintering of the Internet along newly created fault lines. Ahmed and Chander have expressed concern that data nationalism policies to strengthen various sovereign states' economic and socio-political interests is a significant concern for the additional Balkanisation of the Internet.[146] Additionally, Meinrath noted with dismay that the

---

[142] Jonah Force Hill, 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders' [2014] SSRN Electronic Journal <http://www.ssrn.com/abstract=2430275> accessed 15 May 2021.

[143] Chander. A & Uyên P. Lê, 'Data Nationalism', 64 Emory L. J. (2015) at 680- ; Bagchi, Kaushambi; Kapilavai, Sashank, ''Political Economy of Data Nationalism', (22nd Biennial Conference of the International Telecommunications Society (ITS), June 2018)-'.

[144] J Daskal, 'The Un-Territoriality of Data' (2015) 125 Yale Law Journal 326-398, at 330; .Erica Fraser, 'Data Localisation and the Balkanisation of the Internet' (2016) 13 SCRIPTed 359 <https://script-ed.org/?p=3185> accessed 16 May 2021.

[145].Erica Fraser, 'Data Localisation and the Balkanisation of the Internet' (2016) 13 SCRIPTed 359 <https://script-ed.org/?p=3185> accessed 16 May 2021.

[146] Ahmed and Chander, note 2 above, at 1; Chander and Lê,note 1 above, at 680.

increased use of data nationalism policies has led to the global network quickly being transformed into 'various distinct, idiosyncratic 'Internets,' which will result in delays inefficiencies, and higher maintenance and operational costs.[147]

The increased concerns raised by the data nationalism's role in the Balkanisation of the Internet has led to the Organisation for Economic Co-operation and Development (OECD) issuing out a stern warning to states against the imposition of any 'barriers to the location, access and use of cross-border data facilities and functions' in order to 'ensure cost-effectiveness and other efficiencies', in 2011.[148] ECD's warning has since fallen on deaf ears as the decade that followed that warning was wrought with states passing data nationalism policies.[149]

The technical drawbacks of nationalism requirements stand a significant risk of jeopardising the benefits individual users and businesses currently enjoy from integrating global communications and the digital economy into one cornucopia of business needs.[150] These delays will mean real consequences for many eCommerce entities that can only exist because of the existence of the Internet as it currently is. The Internet's division along geopolitical lines also increases the incidence of human rights abuses and political high-handedness.[151]

4.3. The Balkanisation of the Internet and the economy

Data nationalism policies are often regarded as a viable tool to boost domestic economic development and capacity by the imposition of domestic tech solutions and forcing digital entities to have a physical presence in a country. In reality, the wishful thinking of nationalism-inclined policymakers is usually far from the truth. Bauer and Lee-Makiyama have identified several compelling postulations that aid in highlighting the reasoning behind why data nationalism legislation could result in adverse economic effects. The principal of which is the fact that it will result in inefficiencies and cut out smaller markets.[152]

Data nationalism requirements will inevitably result in what can only be described as initial and ongoing increases in costs for end-users, including domestic businesses, as local data services incur significant, service-related, data migration, and infrastructure costs without enjoying the same comparative advantages or efficiencies or economies of scale as global

---

[147] S Meinrath, 'We Can't Let the Internet Become Balkanized' (2013) Slate available at http://www.slate.com/articles/technology/future_tense/2013/10/Internet_balkanization_may_be_a_side_effect_of_the_snowden_surveillance.html (accessed 23 December 2021) Fraser (n 144).

[148] Organisation For Economic Co-operation and Development (OECD), 'OECD Council Recommendation on Principles for Internet Policy Making' (2011) available at http://www.oecd.org/sti/ieconomy/49258588.pdf (accessed 27 December 2021); Chander and Lê, note 1 above, at 722.

[149] Russia, China, Pakistan, and Nigeria have all passed data Nationalism legislations in the past decade Cory and Dascoli (n 44).

[150] Hill, note 2 above, at 49; Hill, note 10 above, at 4; Mishra, note 7 above, at 142; Chander and Lê, note 1 above, at 728-30

[151] Christopher Kuner, 'Data Nationalism and Its Discontents Responses' (2014) 64 Emory Law Journal Online / ELJ Online 2089 at 2090 <https://heinonline.org/HOL/P?h=hein.journals/emyon64&i=89> accessed 9 January 2022. Fraser (n 144).

[152] Matthias Bauer and Hosuk Lee-Makiyama, 'THE COSTS OF DATA LOCALISATION: FRIENDLY FIRE ON ECONOMIC RECOVERY' 20.

businesses.[153] Moreover, services may become unpredictable and unstable if the associated costs of doing business are too exorbitant and the local market is too small to make offering such services an economically sound decision.[154] The result of this forced lack of competition and natural economies of scale is that the local businesses will face difficulties scaling and participating in the global digital economy.[155]

Data nationalism policies are often developed as a strategy to respond to the challenge of 'American Internet hegemony'.[156] Countries intend to utilise data nationalism to ensure their local businesses entities possess a competitive advantage against the big US IT companies present in the country. The intention is that these local companies will eventually increase their share of domestic IT markets otherwise dominated by US IT companies.[157] An example is the Cyber Security Law (CSL) which requires domestic data storage, which by implication also necessitates the establishment of local data centres in mainland China, with the associated investment for infrastructure the creation of jobs locally.[158]

However, there is scepticism about whether data nationalism requirements would benefit domestic economies. Cory noted that their adoption has not led to any considerable increase in the GDP of any states utilising hard data nationalism policies.[159] The economic gains resulting from data nationalism in the domestic economy are usually limited to a few data centres, local enterprises, and ancillary businesses, with a limited number of new vacancies created, and much of the associated IT equipment will likely be still be imported.[160] Those gains are minute in comparison to the significant harms that could befall the remainder of the digital economy.[161]

Secondly, data nationalism laws will reduce access to global IT services for Internet users if business entities decide to limit services to or withdraw from jurisdictions that possess severe restrictions instead of complying.[162] This has a domino effect because it will hinder the ability of domestic businesses to access and build upon relevant technology advancements that include cloud computing[163] and, increasingly, Web3's many innovations. This issue restricts brick and mortar businesses that may want to take advantage of a global eCommerce market from unfettered Internet access.[164] The forced and often hurried establishment of local data centres also possesses several unintended consequences, such as electricity shortages and

[153] ibid.

[154] ibid.

[155] ibid.

[156] Hill (n 142). at 5

[157] Fraser (n 144).

[158] 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)' (n 6).

[159] Nigel Cory, 'The False Appeal of Data Nationalism: Why the Value of Data Comes From How It's Used, Not Where It's Stored' INFORMATION TECHNOLOGY 16. Fraser (n 144).

[160] Fraser (n 144).

[161] ibid.

[162] Tatevik Sargsyan, 'Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security' (2016) 10 International Journal of Communication 17 <https://ijoc.org/index.php/ijoc/article/view/3854> accessed 3 January 2022.

[163] ibid.

[164] ibid.

increases in the costs of electricity consumption that arise as a result of the increased power consumption of the data centres.[165]

Data nationalism restrictions may also hinder international trade.[166] Data nationalism may create an avoidance effect whereby businesses may eschew providing services in the country to avoid compliance, thereby eroding foreign investment.[167] Data nationalism policies also raise the possibility of reciprocal protectionism policies as other countries erect retaliatory trade barriers in response.[168] The end effect will be that consumers will have less choice, and domestic companies will face additional difficulties in expanding globally via the Internet.[169] Furthermore, data nationalism regimes could exclude countries from multilateral trade agreements that preclude hard data nationalism requirements. For instance, Article 14.3 of the Trans-Pacific Partnership (TPP) agreement between the eleven nations along the Pacific Ocean states that '(n)o Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory,' this article is subject to some limited exceptions.[170]

4.4. The Balkanisation of the Internet and human rights concerns

The Internet has become the most crucial tool to communicate with each other globally; additionally, it has broadened what may be termed as individual participation in the political processes. It is also responsible for the increased spotlight on the activities of governments and the promotion and exercising of fundamental rights'.[171] Protests and social uprisings like the Arab Spring, Hong Kong Protests, the #EndSARS protests in Nigeria, and many more would have been impossible to know about, learn from, and support without using the Internet. As a result, information control which has always been the fulcrum of what may be perceived as authoritarian and repressive regimes was facing its biggest challenge from the Internet.[172] Strict data nationalism laws have enabled political oppression and muzzled free speech and the right to protest injustice by consolidating information under governmental control to threaten individual rights such as privacy, data protection, anti-discrimination, freedom of speech, freedom of movement, freedom of association, freedom of expression, and what is now termed as democratic values.[173] For example. Article 40 of the PIPL provides that:

> *Critical information infrastructure operators and personal information handlers who handle personal information up to the amount as specified by the national cyberspace authorities shall store within the territory of the People's*

[165] ibid.

[166] Stephen J Ezell, Robert Atkinson and Michelle A Wein, 'Localization Barriers to Trade: Threat to the Global Innovation Economy' [2013] SSRN Electronic Journal <http://www.ssrn.com/abstract=2370612> accessed 16 May 2021.

[167] ibid.

[168] Determann and others (n 111). Article 42

[169] Ezell, Atkinson and Wein (n 166).

[170] 'TPP Full Text | United States Trade Representative' <https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text> accessed 3 January 2022.

[171] Hill, note 10 above, at 28.

[172] Chander and Lê , note 1 above, at 735.

[173] Kuner, note 12 above, at 2097; Chander and Lê , note 1 above, at 680, 735.

> *Republic of China the personal information which they collect and generate within the territory of the People's Republic of China. If it is really necessary to provide such information overseas, critical information infrastructure operators and personal information handlers shall pass security assessments organised by the national cyberspace authorities; if any law, administrative regulation, or the national cyberspace authorities stipulate that security assessment may not be conducted, such provision shall prevail*.[174]

The effect of the above legislation is that Chinese Social media Giants such as *Weibo* and *WeChat* are beholden to Beijing as opposed to their uses and shareholders as their American counterparts are. The result is Internet tracking and Internet shutdowns which raise concerns about the infringement of the rights to freedom of speech and freedom of expression, as established in Article 19 of the *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights*. This is additionally affirmed by Article 11 of the EU *Charter of Fundamental Rights*.[175]

An open Internet enhances civil liberties because political dissidents have often relied on foreign speech platforms to disseminate information due to the anonymity they offer and the often centralised and government-controlled nature of local speech platforms.[176]
Data nationalism erodes this benefit and ensures that political dissidents are prevented from accessing foreign-based services or, in the alternative, massively throttling the services available to citizens to restrict the flow of information.

Hill notes that while Internet censorship is usually indicated as a significant concern with what many terms authoritarian states, those states deemed as liberal states have also utilised data controls to effectively undermine the civil liberties of their citizens and residents. These liberal states have often cited national security, privacy, law enforcement control, and social-economic reasons to effect data controls.[177] It has become a mainstay of social media since the COVID-19 pandemic began to censor posts deemed misleading by social media companies on the urging of governments.

Many 'liberal' democracies had banned protests since 2020 when the pandemic began, and those restrictions have not yet been overturned two years later. This can have a malignant and dangerous effect because it forms a dangerous precedent that legitimises restrictive data controls. Moreover, liberal countries will have a much weaker position to decry authoritarian regimes' information controls if they are also guilty of using the same tactics.[64]

---

[174] Decree on Management, Provision and Use of Internet Services and Online Information (No. 72/2013), arts 5(1), 24(2) available at http://www.moit.gov.vn/Images/FileVanBan/_ND72-2013CPEng.pdf (accessed on 10 Nov 16).

[175] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III), art 19; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 19; Charter of Fundamental Rights of the European Union, art 11 available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf (accessed 10 Nov 16).

[176] Ahmed, note 2 above, at 2.

[177] Jonah Force Hill, 'A Balkanized Internet?: The Uncertain Future of Global Internet Standards' [2012] Georgetown Journal of International Affairs 49 <http://www.jstor.org/stable/43134338> accessed 16 August 2021.

4.5. The Balkanisation of the Internet and the new surveillance state

The prevention of foreign surveillance and interference within states is one of the most noteworthy justifications for data nationalism laws.[178] It is grounded in the belief that data storage abroad is a threat to privacy and security.[179] The significant consequence of Edward Snowden's exposure of the (National Security Agency's) NSA's systematic violations of individual privacy rights in America and around the world has driven both public and government opinion in favour of legislation that ensure data is kept within national borders to protect individual rights of the citizens of the states and the sovereignty of the state.[180] The US has attracted negative attention for its widespread foreign surveillance activities. However, it is far from the only country running illegal foreign surveillance.[181] The PRC, for example, has been repudiated for using its Tech Giant, *Huawei*, to spy on other countries.[182] Data nationalism requirements have often served as a public repudiation of foreign governments and complicit companies engaged in such tactics.[183]

Despite all the above, it is implausible that data nationalism policies will limit other countries' ability to conduct foreign surveillance activities. For example, the GDPR and the PIPL do not offer complete protection from foreign surveillance since copies of data relating to data subjects present in the EU and Chinese Citizens respectively may be transferred internationally or stored on servers outside the respective countries secretly.[184]

Additionally, the American Government using the Cloud Act, can take possession of data relevant to a crime wherever it is stored upon request by the appropriate law enforcement agency. Thus, data nationalism does not prevent surveillance, as physical access to the data storage or processing facilities is not technically necessary to conduct surveillance activities.[185]

---

[178] G Greenwald and E MacAskill, 'Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data' (2013) The Guardian available at http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining (accessed 8 Nov 16).

[179] Chander and Lê , note 1 above, at 679-80.

[180] Chander and Lê , note 1 above, at 679; N Hopkins, 'UK Gathering Secret Intelligence via Covert NSA Operation' (2013) The Guardian available at http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism (accessed 8 Nov 16); G Greenwald and E MacAskill, 'NSA Prism Program Taps in to User Data of Apple, Google and Others' (2013) The Guardian available at http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (accessed 8 Nov 16).

[181] Greenwald and MacAskill, note 39 above; Chander and Lê , note 1 above, at 715, 717.

[182] 'Huawei Data Flows under Fire in German Court Case' (*POLITICO*, 29 June 2020) <https://www.politico.eu/article/huawei-germany-court-case-privacy/> accessed 10 January 2022; Jürgen Berke, 'Huawei: In China Wissen Sie Alles' <https://www.wiwo.de/my/unternehmen/it/huawei-in-china-wissen-sie-alles/25683032.html> accessed 10 January 2022; News Analysis ANNE MORRIS, Contributing Editor and Light Reading 9/30/2020, 'Germany Stops Short of Huawei Ban, but Raises Bar to Entry' (*Light Reading*) <https://www.lightreading.com/5g/germany-stops-short-of-huawei-ban-but-raises-bar-to-entry/d/d-id/764300> accessed 10 January 2022; Zhou Hanhua, 'Law Expert: Chinese Government Can't Force Huawei to Make Backdoors' *Wired* <https://www.wired.com/story/law-expert-chinese-government-cant-force-huawei-make-backdoors/> accessed 10 January 2022.

[183] Hill, note 10 above, at 23.

[184] Millard, note 4 above, at 4.

[185] Ibid; Chander and Lê , note 1 above, at 715; Daskal, note 17 above, at 369-70. 'CLOUD Act Agreements from an EU Perspective | Elsevier Enhanced Reader' (n 73).

Furthermore, localisation requirements may facilitate foreign surveillance by centralising information in a particular country.

This thereby gives foreign agencies leeway to concentrate surveillance efforts on a few data centres within one geographic entity.[186] The EU avoids the issues that arise from having data centres localised in one geographical entity by ensuring data stored anywhere in the world that falls under the jurisdiction of the GDPR is meant to be treated with the same protection as data stored within Europe.[187]

At the same time, while their governments may claim to denounce foreign surveillance on behalf of their citizens, those same governments that are among the members of the Five Eyes (FVEY)[188] community share information gathered from foreign surveillance.[189] Despite the German Foreign Intelligence Service Bundesnachrichtendienst (BND) and American National Security Agency (NSA) sharing information bilaterally, Germany has criticised the PRISM program and its leading telecom company is considering a localised German-only network.[190] In light of this, data nationalism is not the most efficient method of keeping data away from foreign intelligence agencies.[191] Hill has noted that governments may use data nationalism requirements as a tactic to maximise their bargaining power with foreign intelligence agencies. To the detriment of their data subjects[192] On the other hand, large, global entities possess greater transparency and accountability towards data subjects because the issue notifications, constantly request for consent and make disclosure demands.[193]

---

[186] Chander and Lê , note 1 above, at 717.

[187]Article 1(3) 'EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1'. (n 16).

[188] The Five Eyes is an Anglosphereic intelligence alliance that comprises of Australia, Canada, New Zealand, the United Kingdom, and the United States. These countries are parties to the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence.. J Vitor Tossini, 'The Five Eyes - The Intelligence Alliance of the Anglosphere' (14 April 2020) <https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/> accessed 9 January 2022.

[189] Australia and Canada have imposed data localisation requirements but both programs are limited to health data and National security data. Though it is not expected that it should affect the data sharing obligations.

[190] Editors, ''Prolific Partner': German Intelligence Used NSA Spy Program' (2013) Spiegel Online International available athttp://www.spiegel.de/international/germany/german-intelligence-agenciesused-nsa-spying-program-a-912173.html (accessed 10 Nov 16); F Dohmen and G Traufetter, 'SpyProofing: Deutsche Telekom Pushes for All-German Internet' (2013) Spiegel Online Intternational available at http://www.spiegel.de/international/germany/deutsche-telekom-pushes-all-germanInternet-safe-from-spying-a-933013.html (accessed 10 Nov 16); E MacAskill, J Ball and K Murphy, 'Revealed: Australian Spy Agency Offered to Share Data about Ordinary Citizens' (2013) The Guardian available at http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agencyoffered-to-share-data-about-ordinary-citizens (accessed 10 Nov 16); Chander and Lê , note 1 above, at 716.

[191] Chander and Lê , note 1 above, at 716.

[192] Hill, note 10 above, at 22.

[193] Chander and Lê , note 1 above, at 680; Millard, note 4 above, at 5; Hill, note 10 above at, 21-22, 25-

4.6. The way forward

China has been accused more than once of splintering the Internet because of its data nationalism policies.[194] However, the PRC firmly believes that its objectives are not to balkanise the Internet. Its goals are to control the existing Internet through its governance structure. The PRC's inherent desire is to protect national sovereignty and remedy the demonstrable weakness of the current arrangement in providing security.[195] In the words of *Xi Jinping*, the PRC does not want to create a new separate Internet ringfenced from the rest of the world; instead, it intends to exercise its rights over its cyberspace.[196] These arguments resonate with some countries in Europe because of a widespread belief that American tech giants have adopted a cavalier attitude towards user data and privacy. In non-western countries, they find the tech giants to be unresponsive. The PRC's decision to adopt data nationalism policies has been influenced several other countries, including India, Russia, Vietnam, Nigeria, Brazil, and Pakistan, to adopt hard data nationalism policies.[197]

The point remains to be seen whether the Internet and the digital world could have genuinely been open or accessible. The 'good old days, which are often referenced, were from a time where adoption was not at scale, nor were the uses as diverse. Today, it is a different story, and techno regulation has been one of the ways to curtail the criminality and anarcho-capitalist practices that are rife with the Internet'.[198] Today, tech oligopolies are large enough with enough presence in countries to exercise quasi-governmental powers, which concerns many governments.[199] Zheng notes that Internet search engines already filter results without users' knowledge, and thus, what is made available to the public is only a fraction of the knowledge accessible.[200] Users are confined to digital provinces determined by language and location.[201] Thus, one may ask if the Internet is not already fully Balkanised?

Chander and Lê pointed out that the most significant consequence of Balkanisation is an increase in 'friction,' or in simpler terms, inefficiencies produced by politically constrained connectivity.[202] How difficult will it be to connect as sovereign rule increases? There are precedents. Countries have their currencies, and there are costs to using them in other countries, but it is not impossible. Nations have national telecom service providers, but one can still make international phone calls for a higher fee. The most probable modification from the extension

---

[194] 'The Future of Data Localization and Cross-Border Transfer in China: A Unified Framework or a Patchwork of Requirements?' (n 110).

[195] Pernot-Leplay (n 18).

[196] James Griffiths CNN, 'Chinese President Xi Jinping: Hands off Our Internet' (CNN) <https://www.cnn.com/2015/12/15/asia/wuzhen-china-Internet-xi-jinping/index.html> accessed 3 January 2022.

[197] Cory and Dascoli (n 44). These policies are in various stages with the Russian law being in force since 2019 and the others in vairous stages with the excpectation that by 2023 they will all be laws.

[198] Selby (n 26).

[199] Many governements are considering splitting up big tech entities to avoid a situation where they become a national secutity threat. Ganesh Sitaraman, 'Too Big to Prevail: The National Security Case for Breaking up Big Tech Essays' (2020) 99 Foreign Affairs 116 <https://heinonline.org/HOL/P?h=hein.journals/fora99&i=326> accessed 11 January 2022.

[200] Zheng (n 15); Thomas Lum and Patricia Moloney Figliola, 'China, Internet Freedom, and U.S. Policy' 24.

[201] Zheng (n 59).

[202] Chander. A & Uyên P. Lê, 'Data Nationalism', 64 Emory L. J. (2015) at 680- ; Bagchi, Kaushambi; Kapilavai, Sashank, (n 17).

of data nationalism is increased friction, making it more complex and expensive to connect across borders.

4.7. Accommodating data nationalism

A radical change is inevitable as a result of all these external pressures. To Malcomson, it may be time to, in essence, redefine the ethos and founding principles behind the Internet, as well as the core concepts that underpin its governance and architecture.[203] It is not agreed upon how best to make a reasonable plan of action to others. However, if there is an alternative, it appeals to the interests that initially drove data nationalism. This redefinition must start with an honest and less-romanticised view of the Internet and cyberspace. The redefinition must accommodate the primary concerns of states to protect residents/ citizens without sacrificing fundamental freedoms while addressing the secondary goal for most states to ensure privacy, security, and individual rights in this new space.

Poorly designed and coordinated data control mechanisms ensure that those countries will miss out on the economic, social, and political level playing field arising from digital connectivity to the Internet. Governments will make a political decision to balance the financial cost of regulation against privacy and security benefits. Still, none will decide on actions that lead to significant fracturing. The precedent here is the PRC. PRC's data subjects are often denied access to what others term basic information and have a strange view of events that the Communist Party distorts to serve its interests,[204] but this does not prevent companies' residents in mainland China from doing business.

4.8. Feasibility of a multilateral agreement to circumvent hard data nationalism

Prima facie, it appears highly implausible that the PRC would be willing to commit itself to an agreement that would substantially curtail some of the rights just recently clarified under the CSL, DSL and PIPL. Komatis recognised that the PRC would not consider any moves to permit the transfer or storage of important data out of mainland China as a serious order.[205] Any commitment by the PRC and other countries that have adopted hard data nationalism will need to significantly depend on the severity with which the rules on data transfers to third countries will be enforced by the receiving Data Protection Authorities in the discussed cases. Clear guidance must first be issued to allow the provider to act in accordance with what will now be the law to avoid putting providers and controllers in the middle of a conflict that is politically driven as opposed to economically driven.

Furthermore, in their current form, these Mainland China-based controllers that may fall under the extraterritorial jurisdiction of the GDPR are currently caught between conflicting legal obligations that impose different duties on them. This leaves these businesses in a permanent state of confusion as they may sometimes fail to fulfil some of the obligations they

[203] Reviewed Andrea Miconi, 'Scott Malcomson, SplInternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web, New York and London: OR Books, 2016, 198 Pp., $16.00 (Paperback)'. 4.

[204] Lum and Figliola (n 200).

[205] Konstantinos Komaitis, 'The "Wicked Problem" of Data Localisation' (2017) 2 Journal of Cyber Policy 355 <https://doi.org/10.1080/23738871.2017.1402942>.

ought to.[206] The desire for a standard solution is thus crucial to ameliorate the concerns raised by data nationalism to avoid further Balkanisation of the Internet. A multilateral agreement would be beneficial in this case to address an incidence of an international conflict of laws.

The foremost concern for the existence of such a multilateral agreement is the feasibility of such an agreement. This is a result of the fact that most countries that ought to agree to this agreement strongly believe in the international law principle of sovereignty.[207] Additionally, the distrust that led to data nationalism in the first place has not yet been resolved. The various levels of privacy in various states must also be balanced. The multilateral agreement will involve a level of international participation and cooperation not seen since the United Nations Declaration of Human Rights.[208] The one way to ensure the agreement is feasible is to get the EU, the US and the PRC on board. This can only happen with massive concessions from all three parties and a level of transparency that they have lacked with each other in over a decade. The major driving point for the agreement is that it will give all Nations an opportunity to create a global privacy framework that is universal. This interest must be balanced with the need for states to operate a privacy framework in a vacuum that each state controls through local legislation.

Furthermore, if even two of the aforementioned parties can come to an agreement, enforcement can be ensured through the threat of not recognising the privacy policies of any state that is not a signatory to the multilateral agreement. It is expected that thorough negotiation and mutual compromise will be the deciding factor in the creation of the agreement.

4.9. Essential aspects of a multilateral agreement

The essential aspects that have to be addressed in a multilateral agreement between a hard data nationalism State such as the PRC; a data supremacist state such as the USA, and a state/ body that applies extraterritorial jurisdiction of data such as the EU is that a fair balance must be met between the conflicting laws, rights and political interests between the three systems in order to ensure that there is the free flow of information on the Internet while ensuring there is the protection of the fundamental rights to data protection and privacy.[209]

It is expected that any agreement should acknowledge the importance of data to the world in its recital. It is also expected that the agreement will declare the right to privacy and

---

[206] 'Uncertainty in EU-China Ties Sees Companies Caught between Opportunity and Risk' <https://www.controlrisks.com/campaigns/china-business/uncertainty-in-eu-china-ties-see-companies-caught-between-opportunity-and-risk> accessed 10 January 2022.; Chinese tech company Huwei has so far suffered the brunt of having different privacy protocals in different jurisdictions to great effect; Huwei technology has been all but banned in most of the Five Eyes Member state Nations barring the United Kingdom'Huawei Data Flows under Fire in German Court Case' (n 182); MORRIS, Editor and Reading 9/30/2020 (n 182); Berke (n 182); Hanhua (n 182).

[207] Soveriengty is one of the founding principles of international law; Hans Kelsen, 'Sovereignty and International Law' (1959) 48 Georgetown Law Journal 627 <https://heinonline.org/HOL/P?h=hein.journals/glj48&i=653> accessed 11 January 2022. Martti Koskenniemi, 'The Politics of International Law' (1990) 1 European Journal of International Law 4 <https://heinonline.org/HOL/P?h=hein.journals/eurint1&i=12> accessed 11 January 2022.

[208] United Nations, 'Universal Declaration of Human Rights' (United Nations) <https://www.un.org/en/about-us/universal-declaration-of-human-rights> accessed 11 January 2022.

[209] 'EU Data Localization Would Hurt U.S. Businesses' (The National Law Review) <https://www.natlawreview.com/article/eu-data-localization-would-hurt-us-businesses> accessed 16 August 2021.

set a firm standard expected on the right to privacy as seen in the other rights created in the first, second, and third generation of human rights. Furthermore, it must take great effort to correctly classify data and categorise the data that can be transferred.

4.9.1. Conditions for transferring data

In order to ensure that the fundamental rights of the person affected by a transfer of data are not compromised as the envisaged multilateral agreement, clear conditions for authorising such transfer must be determined. The CSL only provides limited references in this regard, while the GDPR is strict and transparent concerning transfers. The implementing decision adopting standard contractual clauses for the transfer of personal data to third countries, referred to as the new Standard Contractual Clauses (the 'new SCCs'), can be construed as cumbersome in its obligations and vague with regards to the United Kingdom post BREXIT.

Thus, the first step will be to create a global agreement on what transfers are feasible and what is not. For instance, metadata transfers for research and academic purposes should never face restrictions; additionally, transfers relating to pure commerce should not have severe restrictions. This will then need to be domesticated in the local laws of countries.

It is expected that through negotiation, it will be possible to determine what should be considered sensitive data that will face enormous transfer restrictions. This should include health data that is not anonymised and data relating to countries' military and national security architecture. This uniform approach will ensure that all nations are on the same page with each other on the types of data that can and cannot be transferred. Moreover, the definitions should be sufficiently precise in order to avoid any overlaps of data categories, such as, for instance, regarding IP addresses.[210]

4.9.1.1. Restriction of data localisation

One of the major points in any agreement would be the restriction of forced data localisation of all a country's data within its borders. It will be impossible to ensure that data nationalism is not abused to nefarious aims in a situation where one country holds out and guarantees its data is stored locally. The primary reason to store data locally is security. Thus, it makes ample sense to address this concern by setting a uniform standard that will satisfy the concerns of even the most security-conscious nation.[211] Besides, the restriction of data localisation does not mean the end of data nationalism. The agreed-upon sensitive data points can have their data centres stored locally to keep a watchful eye on the relevant data protection offices.

Finally, ensuring that data centres are not stored locally solely will ensure the free flow of information and make it impossible for any nation-state to box off giant data controllers and shake them down on the basis of state-driven interests.

4.9.1.2. Prior judicial review

Although this may lead to conflicting judgments, it is recommended that when the data transfer may be deemed to be ambiguous, the requirement of prior judicial review of cross-

[210] Fraser (n 144).

[211] Cory (n 159).

border transfers will likely be an infringement of the data subjects' rights. It is recommended that for accountability purposes, a court in the country where the data is stored should first grant permission via a simple court order as one would receive for a search warrant before undertaking the transfer. All the judges in such a court must meet a uniform standard. As such, they will need to undertake a qualifying certificate and pass short continuing educational certification before being able to exercise jurisdiction of this sort of case.

4.9.2. Data subject rights and effective judicial remedies

One of the essential aspects of the agreement must be a firm definition of a data subject and an even affirmation of data subjects. All data subjects irrespective of their ethnicity, race or citizenship status within a country must face the same level of protection. For instance, the PIPL is restrictive of the data subjects it protects. At the same time, the EU is *laissez-faire,* with Article 1(4) of the GDPR granting protection to individuals regardless of their citizenship status.

4.10. Conclusion

The EU and the PRC have adopted entirely different attitudes to data nationalism. The result of both hard and soft data nationalism, as seen from the above, remains the Balkanisation of the Internet. Hill notes that due to the concerns of data nationalism, there are now serious discussions on questions about the redesigning of the Internet and a revolutionary adoption of its technical layout and governance structures.[212] Data additionally requires the building and renting of physical infrastructure in the form of data centres in each jurisdiction where the entity has a presence.

The associated operational costs and regulatory burdens that follow that need for physical presence could render the provision of many of the common international services currently taken for granted by Internet users all of a sudden impracticable.[213] Companies may avoid expansion to the developing countries due to a reticence to invest in local infrastructure due to ease of doing business factors, including the possible lack of necessary political stability, supporting laws protecting privacy, data protection, and intellectual property, a good power grid. This may expand the gap in access to technology, innovation and funding for startups.[214] As a result, the increased adoption of data nationalism policies is the biggest threat to the Internet as it currently exists.

The view from the available research is that data nationalism can only be solved at an international level. To this end, such a multi-level agreement that is binding must guarantee an equal level of data protection as under EU and PRC law. In order to serve as a solution, such an agreement must apply to data production as a whole and possess a cross-border context.

It needs to include conditions and safeguards that ensure that the rights of the affected user do not get undermined when data is transferred according to the agreement. The essential aspects to address are the rights of data subjects, the scope of data protection law, conditions

---

[212] Hill, note 10 above, at 4.

[213] Meinrath, note 21 above.

[214] Mishra, note 7 above, at 148; N Lehrer, 'African Datacenters: Understanding Challenges in Emerging Infrastructure in Developing Countries' (2014) available at http://tech.co/africandatacenters-2014-09 (accessed 26 December 2021).

for transfers, restrictions on the forced localisation of data, including prior judicial review before the transfer of data that will be termed illegal. The biggest concern in creating this agreement is the feasibility of the agreement in light of the international law principle of state sovereignty. However, while challenging, that problem can be solved by mutual negotiation and compromise. It is believed that this multi-level agreement will put data nationalism as a relic of the past and ensure that the Balkanisation of the Internet is forestalled.

Chapter V-Conclusion

Countries have seen the inflows of the digital revolution and have decided to take a proactive regulatory standpoint to what is termed the new oil of the digital revolution, data. For a myriad of reasons including, the need to protect the sovereign interests of its citizens, countries have taken up a firm and what is termed a nationalism stance to data by ensuring data of a country should either be stored within the country's borders; or face restrictions in transfers.

These policies are resulting in the splintering of the digital hegemony of what we know today as the Internet. This splintering is termed the Balkanisation of the Internet, and it raises serious, legal, regulatory and business-related concerns. Indeed, the significant concerns include threats of Internet censorship and human rights abuses, restrictions in the free access of information, difficulty in digital businesses to scale to different countries efficiently, and a more expensive and less efficient digital space.

Nonetheless, this thesis has demonstrated that the *opinio juris* among the European Union and the People's Republic of China continues to regard such data nationalism measures as necessary for protecting the state and the citizens. In particular, the European Union (EU), General Data Protection Regulation 2016/679 (GDPR), Personal Information Protection Law of the People's Republic of China (PIPL) and the Data Security Law of the People's Republic of China (DSL), which hitherto remains the most significant municipal data protection legislation in the European Union and the People's Republic of China respectively provide strong backing for data nationalism policies that mandate transfer restrictions and the localisation of data in various instances.

The scope of this thesis was limited to the analysis of data nationalism in the EU and the PRC. Furthermore, this thesis addressed the issue primarily from a personal data protection perspective. The legal questions regarding cybercrime and eCommerce were not touched upon beyond analysing issues that aided in answering the research questions.

The EU's approach to data nationalism is driven by the EU policy to protect the human rights of every individual present in the EU regardless of citizenship or residency status. The GDPR in Chapter V regulates data transfers and ensures that data outflows from the European Economic Area (EEA) are done within several specific contexts. It set an explicit limitation on the transfer of data to either country with adequate protection in Article 45, or countries with appropriate safeguards in Article 46 and countries with binding contractual rules in article 47. However, there is an opportunity for derogations in specific contexts. The EU's stance on data nationalism has now been defined as soft data nationalism.

Additionally, the EU also possesses what is termed as extraterritorial jurisdiction through the interpretation of Article 3(2) of the GDPR. It is a practice by which the EU ensures it enforces its data policy beyond its borders by possessing jurisdiction against foreign entities that are not resident within the EU but fall under the jurisdiction of the GDPR because they process data belonging to European data subjects or specifically target European data subjects. This puts such companies in a difficult position since those subsidiaries are bound as well by the GDPR's and PIPL's limitations on data transfers to third countries.

The territorial scope of the GDPR, on the other hand, equally entails extraterritorial effects, also obliging data controllers solely established outside the EU. In essence, the approaches under the GDPR are a clear example of lawmakers' attempts to establish

jurisdiction over online services, regardless of traditional territorial boundaries. Irrespective of these GDPR positions, the EU approach to data is still very *laissez-faire* in practice, and the data nationalism in the EU is termed soft.

The People's Republic of China (PRC) has taken a different approach to data nationalism. Chapter 3 of the PIPL has set rules for providing personal information out of mainland China. Articles 38 – 43 of the PIPL have additionally imposed rules relating to data transfers and localisation, with some restrictions. Data pertaining to critical information infrastructure operators ('CIIOs') and some big personal information processors must be localised in mainland China under Article 40 of the PIPL.

In comparison, there is a censure of information in Article 41 of the PIPL, which requires that personal information processors shall not provide personal information to foreign public authorities without obtaining the permission of the competent Chinese authority. Reciprocity is a huge part of the PIPL, and in Article 42, the Cyberspace Administration of China (CAC) is authorised to build up a restricted and prohibited list of personal information transfers for organisations or individuals outside of mainland China that infringe a Chinese citizen's personal information, or process personal information to damage the national security or public interest.

Furthermore, Article 43 requires the adoption of reciprocal actions for any discriminatory prohibitions, restrictions, or other similar measures against the PRC made by any country or region in terms of personal information protection. The major criticism of the PIPL and other PRC legislation is the lack of clarity on several terms and policies mentioned throughout the laws, including the term 'important data'. The PRC position is an example of hard data nationalism in play. The PRC is also guided by the need to exhibit state supremacy over data subjects. The two systems mentioned are opposites in practice and administration, but they are the two major templates for deciding data policies worldwide.

Regardless of the concerns about the conformity of EU and the PRC legislation to businesses, the two pieces of legislation are nonetheless binding to all companies involved in controlling and processing data in those jurisdictions and affect their subsidiaries on foreign territories. The legal position of the EU and the PRC has led to some difficulties for businesses in scaling properly because forced localisation and transfer restrictions create a barrier for entry that many startups and eCommerce entities will not be able to overcome. It is also a significant concern that access to the Internet will become more expensive due to localisation requirements.

Furthermore, technological innovations like Cloud Technology and the decentralised Internet will not thrive adequately with localisation requirements. Moreover, data nationalism tends to lead to human rights concerns since the states will have avenues to shut down critical data points that are stored locally at a whim to the detriment of the data subjects. This has risen in significance with the increased Internet shutdowns within states and the restrictions of data inflows during protests. Additionally, there are significant concerns that data nationalism will increase the incidence of illegal surveillance on data subjects and other sovereign states due to the government having seamless access to data centres.

This thesis has found that all these concerns do not exist individually but accumulate to increase concerns on the issue that data nationalism contributes to the Balkanisation of the Internet. Whereas this conflict could be resolved by reviewing the data nationalism policies of

the PRC and the EU separately and amending the GDPR and PIPL to allay fears, this problem is an international problem exacerbated by extraterritorial concerns, which therefore deserves an international solution.

To that end, this thesis has focused on the possibility of a multilateral international agreement between the EU, the PRC, and the United States of America (USA) as a solution. That agreement will be the groundwork for an international data protection law with uniform standards. This solution was selected as most preferable based on the global reach of the Internet and the large number of transnational data crossflows which will need to be permitted to continue on an international level that involves as many countries as possible.

This will limit the spread of strict data nationalism requirements that currently threaten the openness of the Internet as such. The feasibility of such an agreement is one of the major concerns. The three mentioned states all possess different types of data policies and enforce data regulations in different ways. The only feasible way to bring them to an agreement is to ensure the agreement makes enough compromises to allay the fears and concerns of all while protecting the existing rights and interests and giving opportunity for much-needed freedoms into new markets.

From a data protection perspective, the following recommendations should thus be considered when drafting a multilateral agreement:

- The data categories which are encompassed by the agreement should be clearly defined in order to provide legal certainty and clarity.

- The rights of data subjects should be clearly defined and put as one of the guiding principles

- The scope of data protection principles in the agreement includes the limitations to what is covered in order to protect national security interests

- The conditions for transfers restrictions where the need arises and the identification of the limited cases where forced localisation of data will be permitted

- The including prior judicial review before the transfer of data that will be termed illegal

Finally, the problem of data nationalism should not be taken lightly. It is also not a problem with easy solutions as the solutions involve building trust amongst nations that do not seem to trust each other again. This thesis has taken great lengths to understand the concept better as well as classifying it into different forms will aid in identifying what it is and what it is not. The concept of data nationalism has led to a splintering of the one Internet in what is now termed the Balkanisation of the Internet, which raises serious human rights and economic concerns for data subjects and businesses that are either startups or multinationals with a presence in several countries.

Data nationalism can be addressed by mutual negotiation and compromise and the drawing up of a multilateral agreement that addresses the concerns of all signatories while creating an avenue for the seamless cross-border transfer of data. It is believed that this multi-

level agreement will put data nationalism as a relic of the past and ensure that the Balkanisation of the Internet is forestalled.

Bibliography

Primary Sources

Legislation

Data Security Law of the Peoples Republic of China (2021) Article 36 '中华人民共和国数据安全法' (China Law Translate, 10 June 2021) <https://www.chinalawtranslate.com/datasecuritylaw/> accessed 31 October 2021.

Personal Information Protection Law of the People's Republic of China (Chairman's Order No. 91) (the PIPL) 2021
Cyber Security Law of the People's Republic of China (2017)

'EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council on 27 April 2016 on the Protection of Natural Persons with Regards to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1'. (General Data Protection Regulation (GDPR)).

Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

Directive 2000/31/EC of the European Parliament and of the Council on 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on Electronic Commerce') 'EUR- Lex- 32000L0031- EN' (Official Journal L 178, 17/07/2000 P. 0001- 0016).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 124 Schrems (n 20).

European Union Law

Public Records Act, 1995.

Legislative Proposals by the European Union

Commission, 'Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data'.
Data Protection Working Party, 'Statement on Data Protection and Privacy Aspects of Crossborder Access to Electronic Device' (2017) 4 28 Commission (n 25) 6.

US Statutory Law
H.R. 4943- Cloud Act 115th Congress (2017-2018).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, 2001.

International Treaties

International Covenant on Civil and Political Rights. Adopted by the General Assembly of the United Nations on 19 December 1966.

The United Nations, Declaration on the Rights of Indigenous Peoples of the General Assembly, A/RES/ 61/295.

Universal Declaration of Human Rights (Adopted 10 December 1948 UNGA Res 217 A (III).

Case Law

Court of Justice of the European Union

Data Protection Commissioner v *Facebook Ireland Ltd and Maximilian Schrems ('Schrems II')* (2020) C-311/ 18.

Maximilian Schrems v *Data Protection Commissioner [GC]* (2015) C- 362/14.

Schrems v *Data Protection Commissioner* [2014] IEHC 310 (IEHC).

Soriano v *Forensic News LLC & Ors* [2021] EWHC 56 (QB).

Weltimmo v *Nemzeti Adatvdelemi es Informacioszabadsag Hatosag* [2015] Court of Justice of the EU Judgment (C-230/14), ECLI: EU: C: 2015:639 ECLI: 639.

Supreme Court of the United States

United States v *Microsoft Corp.* 584 U.S. 138 S. Ct. 1186.

Secondary Sources

Official EU Documents

European Commission

'Adequacy Decisions' (*European Commission- European Commission)*

'EUR-Lex – 32000L0031- EN'(*Official Journal L 178, 17/07/2000 P. 0001-0016).*

European Data Protection Board

European Data Protection Board, 'Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data'.

United Nations

The United Nations Conference on Trade and Development Secretariat, 'The Value and Role of Data in Electronic Commerce and Digital Economy and its Implication for Inclusive Trade and Development' (2019) Trade and Development Board Intergovernmental Group of Experts on E-Commerce and the Digital Economy Third Session Geneva, at 18.

United Nations High Commissioner for Refugees, 'European Union, Directive 95/46/EC of the European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1945.

World Intellectual Property Organization, 'The Mataatua Declaration on Cultural and Intellectual Property Rights of Indigenous Peoples'.

Books

B. Kaushambi and K. Sashank, *Political Economy of Data Nationalism*, (22nd Biennial Conference of the International Telecommunications Society (ITS), June 2018)'.

Higgins V, *The Perils of Strategic Technological Development Policy: Two Failed Chinese Attempts, FDI and Techno-Nationalism.* In: Alliance Capitalism, Innovation and the Chinese State. International Political Economy Series. (Palgrave Macmillan UK 2015).

Hon WK, *Data Localization Laws and Policy : The EU Data Protection International Transfers Restriction through a Cloud Computing Lens* (Edward Elgar Publishing Limited 2017).

Miconi RA, Malcomson S., *Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web*, (New York and London: OR Books, 2016).

Tapscott D, *The Digital Economy: 20th Anniversary Edition: Rethinking Promise and Peril in the Age of Networked Intelligence* (McGraw Hill; 2nd edition October 28, 2014).

Todora M N, *Imagining the Balkans* (Updated ed, Oxford University Press 2009).

Ursic H et al, *Research Handbook on Data Science and Law* (Edward Elgar Publishing 2018).

Online Sources

'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)' (*New America*, 29 June 2018) http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ accessed 16 August 2021.

Capri A., 'Techno-Nationalism: What Is It and How Will It Change Global Commerce?' (*Forbes*, 20 December 2019) https://www.forbes.com/sites/alexcapri/2019/12/20/techno-nationalism-what-it-is-and-how-will-it-change-global-commerce/?sh=273c0032710f accessed 20 January 2022.

Chander A., Is Data Localization a Solution for Schrems II? (2020). *Journal of International Economic Law*, Forthcoming,

SSRN: https://ssrn.com/abstract=3662626 or http://dx.doi.org/10.2139/ssrn.3662626 accessed 20 January, 2022.
Chander. A & Uyên P. Lê, 'Data Nationalism' (2015) 64(3) *Emory Law Journal* 677. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2 accessed 20 January, 2022.
Chen J and Sun J, 'Understanding the Chinese Data Security Law' (2021) 2 International Cybersecurity Law Review https://doi.org/10.1365/s43439-021-00038-3 accessed 4 January 2022.
Cory N and Dascoli L, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them' (*Information and Technology Innovation Foundation*, 19 July 2021) https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost accessed 20 January, 2022.
Cory N., 'The False Appeal of Data Nationalism: Why the Value of Data Comes From How It's Used, Not Where It's Stored' (*Information Technology and Innovation Foundation*, 1 April 2019) https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where accessed 20 January, 2022.
Hill J., 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders' [2014] *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance*, http://www.ssrn.com/abstract=2430275 accessed 15 May 2021.
Hill JF, 'A Balkanized Internet?: The Uncertain Future of Global Internet Standards' [2013] *Georgetown Journal of International Affairs* < https://www.georgetownjournalofinternationalaffairs.org/online-edition/a-balkanized-internet-the-uncertain-future-of-global-internet-standards-by-jonah-force-hill> accessed 16 August 2021.
Kuner C., 'Data Nationalism and Its Discontents Responses' (2014) 64 *Emory Law Journal Online / ELJ Online* 2089 https://heinonline.org/HOL/P?h=hein.journals/emyon64&i=89 accessed 9 January 2022.
Lou Y et al, 'The Future of Data Localization and Cross-Border Transfer in China: A Unified Framework or a Patchwork of Requirements?' (*Iapp News*, 22 June 2021) https://iapp.org/news/a/the-future-of-data-localization-and-cross-border-transfer-in-china-a-unified-framework-or-a-patchwork-of-requirements/ accessed 31 October 2021.
Lum T and Figliola PM, 'China, Internet Freedom, and U.S. Policy' https://sgp.fas.org/crs/row/R42601.pdf accessed 20 January, 2022.
Malcomson S., 'Welcome to the Splinternet' (*Techonomy*, 22 December 2015) https://techonomy.com/2015/12/welcome-to-the-splinternet/ accessed 16 August 2021.
MORRIS NAA, Editor C and Reading 9/30/2020 L, 'Germany Stops Short of Huawei Ban, but *Management* 1231 https://linkinghub.elsevier.com/retrieve/pii/S0268401216304753 accessed 14 May 2021.
Zhang L and others, 'A Review of Open Research Data Policies and Practices in China' (2021) 20 *Data Science Journal* 3 http://datascience.codata.org/articles/10.5334/dsj-2021-003/ accessed 13 December 2021.
Zheng H, 'Regulating the Internet: China's Law and Practice' (2013) 04 *Beijing Law Review* 37 http://www.scirp.org/journal/doi.aspx?DOI=10.4236/blr.2013.41005 accessed 14 May 2021.